

que deben ser consideradas aplicar al mismo. Se elabora también el formulario de necesario para realizar la solicitud de un cambio.

21.2. Formalización del "Proceso de Registro y Resolución de errores": el proceso es evaluado y aprobado por el comité de seguridad de la información. Posteriormente se formaliza el mismo (se distribuye el documento a las personas que corresponda)

21.3. Capacitación: se capacita al personal involucrado en el proceso con el propósito de que las tareas sean realizadas conforme a lo establecido previamente

22. Sincronización del reloj

22.1. Configuración del reloj en las computadoras del hospital: Se procede a configurar el reloj de las computadoras de usuario, de manera tal que estos estén sincronizados con el reloj del servidor de la institución.

4.5.11.3 *Estimación de tiempos*

Seguidamente, se establecen los tiempos y recursos para cada una de las actividades previamente detalladas

UCS - Facultad de Ingeniería  
Revisión de los Procesos de Seguridad del Hospital Dr. Arturo Oñativia  
Solución Propuesta

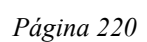
|    | Nombre                                                               | Duración | Predeterminación | Recursos                                                                             |
|----|----------------------------------------------------------------------|----------|------------------|--------------------------------------------------------------------------------------|
| 1  | ☐Gestión de las Comunicaciones y Operaciones                         | 233.33d  |                  |                                                                                      |
| 2  | Inicio de tareas de Seguridad de los Recursos Humanos                | 0h       |                  |                                                                                      |
| 3  | ☐Procedimientos y responsabilidades operativas                       | 24.67d   |                  |                                                                                      |
| 4  | ☐Documentación de los procedimientos operativos                      | 12.83d   |                  |                                                                                      |
| 5  | Elaboración de la documentación de procedimientos operativos         | 60h      | 7                | Responsable de Seguridad de la Información, Persona del Sector de Sist. Inf.         |
| 6  | Formalización de la documentación elaborada                          | 6h       | 5                | Comité de Seguridad de la Información                                                |
| 7  | ☐Gestión de cambios                                                  | 9.67d    |                  |                                                                                      |
| 8  | Documentación del "Proceso de Gestión de Cambios"                    | 12h      | 5                | Responsable de Seguridad de la Información, Jefe del Sector de Sistemas Informáticos |
| 9  | Formalización del "Proceso de Gestión de Cambios"                    | 3h       | 15.8             | Comité de Seguridad de la Información                                                |
| 10 | Actualización de la Política de Seguridad                            | 3h       | 9                | Responsable de Seguridad de la Información                                           |
| 11 | Capacitación                                                         | 3h       | 9                | Jefe del Sector de Sistemas Informáticos                                             |
| 12 | ☐Separación de las instalaciones de desarrollo, de pruebas y operaci | 5d       |                  |                                                                                      |
| 13 | Construcción de la Base de Datos de Prueba                           | 30h      | 11               | Persona del Sector de Sist. Inf.                                                     |
| 14 | ☐Gestión de la entrega de servicios por terceras partes              | 1d       |                  |                                                                                      |
| 15 | Actualización de la Política de Seguridad                            | 6h       | 10               | Responsable de Seguridad de la Información                                           |
| 16 | ☐Planificación y aceptación de sistemas                              | 1d       |                  |                                                                                      |
| 17 | Actualización de la Política de Seguridad                            | 6h       | 15               | Responsable de Seguridad de la Información                                           |
| 18 | ☐Protección contra código malicioso y código móvil.                  | 22d      |                  |                                                                                      |
| 19 | ☐Controles contra código malicioso                                   | 22d      |                  |                                                                                      |
| 20 | ☐Instalación del Firewall                                            | 16d      |                  |                                                                                      |
| 21 | Instalación y Configuración en Ambiente de Prueba                    | 24h      | 11,17            | Responsable de Seguridad de la Información, Jefe del Sector de Sistemas Informáticos |
| 22 | Pruebas                                                              | 90h      | 21               | Responsable de Seguridad de la Información, Jefe del Sector de Sistemas Informáticos |
| 23 | Instalación y Configuración en el Ambiente de Producción             | 12h      | 22               | Responsable de Seguridad de la Información, Persona del Sector de Sist. Inf.         |
| 24 | ☐Instalación del Antivirus Empresarial                               | 6d       |                  |                                                                                      |
| 25 | Instalación y Configuración en el Ambiente de Producción             | 12h      | 23               | Responsable de Seguridad de la Información, Jefe del Sector de Sistemas Informáticos |
| 26 | Instalación del antivirus en los equipos de tipo "cliente"           | 24h      | 13,25            | Persona del Sector de Sist. Inf.                                                     |
| 27 | ☐Controles contra código móvil                                       | 0.5d     |                  |                                                                                      |
| 28 | Actualización de la Política de Seguridad                            | 3h       | 25               | Responsable de Seguridad de la Información                                           |
| 29 | ☐Resguardo                                                           | 22.67d   |                  |                                                                                      |
| 30 | ☐Resguardo de la información                                         | 22.67d   |                  |                                                                                      |
| 31 | Elaboración de la política de resguardo                              | 30h      | 25,26            | Responsable de Seguridad de la Información, Jefe del Sector de Sistemas Informáticos |
| 32 | Formalización de la política de resguardo                            | 12h      | 31               | Comité de Seguridad de la Información                                                |
| 33 | Actualización de la Política de Seguridad                            | 4h       | 32               | Responsable de Seguridad de la Información                                           |
| 34 | Adquisición de medio de almacenamiento y caja fuerte ignífuga        | 60h      | 32               | Personal del Sector de Compras                                                       |
| 35 | ☐Gestión de la seguridad de la red                                   | 6d       |                  |                                                                                      |
| 36 | ☐Controles de redes                                                  | 0.83d    |                  |                                                                                      |
| 37 | Ampliar Documentos de Visión, Misión y Funciones de Sector de Sist.  | 6h       | 32               | Comité de Seguridad de la Información                                                |
| 38 | ☐Seguridad de los servicios de red                                   | 0.5d     |                  |                                                                                      |
| 39 | Actualización de la Política de Seguridad                            | 2h       | 33               | Responsable de Seguridad de la Información                                           |
| 40 | ☐Manejo de medios                                                    | 89.67d   |                  |                                                                                      |
| 41 | ☐Gestión de medios removibles                                        | 14.33d   |                  |                                                                                      |
| 42 | Documentación del "Proceso para la gestión de Medios Removibles"     | 12h      | 37               | Comité de Seguridad de la Información                                                |
| 43 | Formalización del "Proceso para la gestión de Medios Removibles"     | 3h       | 42               | Comité de Seguridad de la Información                                                |

Ilustración 4.5-23

UCS - Facultad de Ingeniería  
Revisión de los Procesos de Seguridad del Hospital Dr. Arturo Oñativia  
Solución Propuesta

|    |                                                                                                 |         |                  |                                                                                      |
|----|-------------------------------------------------------------------------------------------------|---------|------------------|--------------------------------------------------------------------------------------|
| 44 | Actualización de la Política de Seguridad                                                       | 3h      | 39.43            | Responsable de Seguridad de la Información                                           |
| 45 | Capacitación                                                                                    | 3h      | 41               | Miembro del Comité de Seguridad                                                      |
| 46 | <input checked="" type="checkbox"/> Eliminación de Medios Removibles                            | 14.17d  |                  |                                                                                      |
| 47 | Documentación del "Proceso para la eliminación de Medios"                                       | 12h     | 43               | Comité de Seguridad de la Información                                                |
| 48 | Formalización del "Proceso para la eliminación de Medios"                                       | 3h      | 47               | Comité de Seguridad de la Información                                                |
| 49 | Actualización de la Política de Seguridad                                                       | 2h      | 44.48            | Responsable de Seguridad de la Información                                           |
| 50 | Capacitación                                                                                    | 3h      | 45.48            | Miembro del Comité de Seguridad                                                      |
| 51 | <input checked="" type="checkbox"/> Procedimientos para el manejo de la información             | 56.33d  |                  |                                                                                      |
| 52 | Elaboración y formalización del registro de personal autorizado                                 | 50h     | 48               | Comité de Seguridad de la Información                                                |
| 53 | Actualización de la Política de Seguridad                                                       | 4h      | 49.52            | Responsable de Seguridad de la Información                                           |
| 54 | Elaboración de guía para el uso y cuidado de medios removibles                                  | 12h     | 53               | Responsable de Seguridad de la Información, Jefe del Sector de Sistemas Informáticos |
| 55 | <input checked="" type="checkbox"/> Intercambio de la información                               | 74.17d  |                  |                                                                                      |
| 56 | <input checked="" type="checkbox"/> Políticas y Procedimientos de Intercambio de la Información | 5d      |                  |                                                                                      |
| 57 | Concientización                                                                                 | 30h     | 54               | Responsable de Seguridad de la Información                                           |
| 58 | <input checked="" type="checkbox"/> Acuerdos de intercambio                                     | 30d     |                  |                                                                                      |
| 59 | Documentación del "Proceso de Solicitud e Instalación de Firma Digital"                         | 12h     | 52               | Comité de Seguridad de la Información                                                |
| 60 | Formalización del "Proceso de Solicitud e Instalación de Firma Digital"                         | 6h      | 59               | Comité de Seguridad de la Información                                                |
| 61 | Actualización de la Política de Seguridad                                                       | 3h      | 57.60            | Responsable de Seguridad de la Información                                           |
| 62 | Capacitación                                                                                    | 60h     | 50.60            | Miembro del Comité de Seguridad                                                      |
| 63 | <input checked="" type="checkbox"/> Medios Físicos en tránsito                                  | 7.17d   |                  |                                                                                      |
| 64 | Elaboración del documento para el transporte de medios                                          | 12h     | 61               | Responsable de Seguridad de la Información                                           |
| 65 | Formalización del documento para el transporte de medios                                        | 6h      | 60.64            | Comité de Seguridad de la Información                                                |
| 66 | Actualización de la Política de Seguridad                                                       | 3h      | 65               | Responsable de Seguridad de la Información                                           |
| 67 | Adquisición del medio de protección                                                             | 30h     | 34.64            | Personal del Sector de Compras                                                       |
| 68 | <input checked="" type="checkbox"/> Mensajería electrónica                                      | 16d     |                  |                                                                                      |
| 69 | Instalación y Configuración en Ambiente de Prueba                                               | 24h     | 54.66            | Responsable de Seguridad de la Información, Jefe del Sector de Sistemas Informáticos |
| 70 | Pruebas                                                                                         | 60h     | 60               | Responsable de Seguridad de la Información, Jefe del Sector de Sistemas Informáticos |
| 71 | Instalación y Configuración en el Ambiente de Producción                                        | 12h     | 70               | Responsable de Seguridad de la Información, Jefe del Sector de Sistemas Informáticos |
| 72 | <input checked="" type="checkbox"/> Sistema de información del negocio                          | 41.17d  |                  |                                                                                      |
| 73 | Elaboración de la política de intercambio                                                       | 30h     | 65               | Comité de Seguridad de la Información                                                |
| 74 | Formalización de la política de intercambio                                                     | 12h     | 73               | Comité de Seguridad de la Información                                                |
| 75 | Actualización de la Política de Seguridad                                                       | 2h      | 71.74            | Responsable de Seguridad de la Información                                           |
| 76 | <input checked="" type="checkbox"/> Seguimiento y Control                                       | 189.67d |                  |                                                                                      |
| 77 | <input checked="" type="checkbox"/> Registro de auditoría                                       | 10d     |                  |                                                                                      |
| 78 | Modificación de los registros de auditoría                                                      | 60h     | 26               | Personal del Sector de Sist. Inf.                                                    |
| 79 | <input checked="" type="checkbox"/> Protección de la inf. de los registros de actividad         | 2.5d    |                  |                                                                                      |
| 80 | Elaboración de normativa interna                                                                | 12h     | 75               | Responsable de Seguridad de la Información, Jefe del Sector de Sistemas Informáticos |
| 81 | Capacitación                                                                                    | 3h      | 80               | Responsable de Seguridad de la Información                                           |
| 82 | <input checked="" type="checkbox"/> Registros de acciones fallidas                              | 4.63d   |                  |                                                                                      |
| 83 | Documentación del "Proceso de Registro y Resolución de errores"                                 | 12h     | 80               | Jefe del Sector de Sistemas Informáticos                                             |
| 84 | Formalización del "Proceso de Registro y Resolución de errores"                                 | 6h      | 74.83            | Comité de Seguridad de la Información                                                |
| 85 | Capacitación                                                                                    | 3h      | 84               | Jefe del Sector de Sistemas Informáticos                                             |
| 86 | <input checked="" type="checkbox"/> Sincronización del reloj                                    | 12h     |                  |                                                                                      |
| 87 | Configuración del reloj en las computadoras del hospital                                        | 12h     | 78               | Personal del Sector de Sist. Inf.                                                    |
| 88 | Fin de tareas de Gestión de Activos                                                             | 0d      | 62.87, 81.85, 87 |                                                                                      |

Ilustración 4.5-24



## 4.5.12 Análisis de Riesgos.

Se establecen los riesgos a los que está expuesta la institución al no realizar una adecuada gestión de las Comunicaciones y operaciones.

| <u>Riesgo</u>                                                                 | <u>Impacto</u> | <u>Probabilidad</u> | <u>Importancia</u> | <u>Prevención</u>                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------|----------------|---------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u>Fuga de información</u>                                                    | <u>10</u>      | <u>0,5</u>          | <u>5</u>           | <u>Apropiados acuerdos de seguridad de la información con terceras partes.</u><br><u>Seguimiento y control de los servicios prestados por terceros.</u><br><u>Adecuado proceso para la gestión y eliminación de medios removibles</u><br><u>Adecuados procesos para el manejo e intercambio de información</u><br><u>Correcta protección de los medios en tránsito (protección de la información en tránsito)</u> |
| <u>Ataque de código malicioso a la infraestructura tecnológica</u>            | <u>7</u>       | <u>0,2</u>          | <u>1,4</u>         | <u>Firewall UTM.</u><br><u>Antivirus Empresarial.</u>                                                                                                                                                                                                                                                                                                                                                             |
| <u>Riesgo de phishing y spam</u>                                              | <u>2</u>       | <u>0,6</u>          | <u>1,2</u>         | <u>Firewall UTM.</u><br><u>Servidor de mensajería electrónica</u><br><u>Servidor LPDA</u>                                                                                                                                                                                                                                                                                                                         |
| <u>Daño o alteración de la información debido a cambios mal implementados</u> | <u>3</u>       | <u>0,2</u>          | <u>0,6</u>         | <u>Apropiado proceso para la gestión de cambios en los sistemas de información</u>                                                                                                                                                                                                                                                                                                                                |

|                                            |                  |                    |                   |                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------|------------------|--------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <u><b>Pérdida total de información</b></u> | <u><b>10</b></u> | <u><b>0,05</b></u> | <u><b>0,5</b></u> | <u><b>Adecuada política de resguardo de la información</b></u><br><br><u><b>Apropiados Procesos para la gestión de medios removibles</b></u><br><br><u><b>Correcto manejo de los medios en tránsito (medios removibles en tránsito)</b></u><br><br><u><b>Firewall UTM.</b></u><br><br><u><b>Antivirus Empresarial.</b></u> |
|--------------------------------------------|------------------|--------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Tabla 4.5-30

#### 4.5.13 Análisis Económico-Financiero

##### 4.5.13.1 Estimación de costos.

A continuación, se detallan los costos necesarios para implementar las mejoras propuestas

- Hardware: En cuanto a costos de Hardware, se registra la adquisición de 2 discos duros externos mencionados en (**Resguardo de la inf**)

| HARDWARE                 |          |                 |          |
|--------------------------|----------|-----------------|----------|
| ITEM                     | CANTIDAD | PRECIO UNITARIO | TOTAL    |
| Disco duro externo (1Tb) | 2        | \$ 1.500        | \$ 3.000 |
| Total                    | \$ 3.000 |                 |          |

Tabla 4.5-31

- Equipamiento: Se registran en este concepto la adquisición de una caja fuerte ignífuga (mencionada en **Resguardo de la información**), y la compra de 2 contenedores (maletines) impermeables (ver **Medios Físicos en tránsito** ).

| Equipamiento           |          |                 |          |
|------------------------|----------|-----------------|----------|
| ITEM                   | CANTIDAD | PRECIO UNITARIO | TOTAL    |
| Contenedor Impermeable | 2        | \$ 1.500        | \$ 3.000 |

|                      |                  |           |           |
|----------------------|------------------|-----------|-----------|
| Caja fuerte ignífuga | 1                | \$ 10.000 | \$ 10.000 |
| <b>Total</b>         | <b>\$ 13.000</b> |           |           |

Tabla 4.5-32

- Software: Se registra la adquisición de las licencias de un antivirus empresarial, mencionado en **Código malicioso**

| SOFTWARE                          |                     |                 |                             |
|-----------------------------------|---------------------|-----------------|-----------------------------|
| ITEM                              | CANTIDAD            | PRECIO UNITARIO | COSTO ANUAL                 |
| Licencia empresarial de antivirus | 140                 | \$ 327,34       | \$ 45.827,60 <sup>114</sup> |
| <b>Total</b>                      | <b>\$ 45.827,60</b> |                 |                             |

Tabla 4.5-33

- Recursos Humanos: Debido a que el personal de la Institución es el encargado de llevar adelante las tareas anteriormente mencionadas, no se registran costos en este concepto.

| Costos Totales |                  |
|----------------|------------------|
| Ítem           | Precio           |
| Hardware       | \$ 3.000         |
| Software       | \$ 0             |
| Equipamiento   | \$ 13.000        |
| <b>TOTAL</b>   | <b>\$ 16.000</b> |

Tabla 4.5-34

<sup>114</sup> Valores cotizados por la empresa McAfee al día de la fecha (24/08/2016), a través del siguiente link:  
[http://www.shopmcafee.com.ar/store/mfesmb/es\\_MX/pd/productID.306911700/categoryID.66300400](http://www.shopmcafee.com.ar/store/mfesmb/es_MX/pd/productID.306911700/categoryID.66300400)  
 Yustman, Mauricio Ezequiel

| Costos Anuales |                     |
|----------------|---------------------|
| Ítem           | Precio              |
| Hardware       | \$ 0                |
| Software       | \$ 45.827,60        |
| Equipamiento   | \$ 0                |
| <b>TOTAL</b>   | <b>\$ 45.827,60</b> |

Tabla 4.5-35

#### 4.5.13.2 Beneficio Operativos

La implementación de la solución propuesta brindará los siguientes beneficios a la institución:

- Asegurar que los cambios realizados en los sistemas de información no afecten al funcionamiento de los mismos. Mediante la apropiada gestión de cambios aseguramos la integridad y disponibilidad de la información del sistema.
- Aumento de la cultura de cuidado de la información institucional. Mediante apropiadas políticas de resguardo y procesos de manejo de la información.
- Reducción de la probabilidad de pérdida de información generada por un inapropiado manejo de la información, incorrectos procesos de custodia para la información en tránsito, inadecuadas políticas de intercambio de información o por problemas ocasionados por terceros.
- Administración unificada de la seguridad de la red institucional. El Firewall UTM provee de una herramienta a partir de la cual es posible disminuir los problemas causados por software malintencionado. El firewall es una herramienta con la que podemos mejorar el rendimiento de las redes.
- Eficiencia en la gestión de la mensajería electrónica. El servidor de correo permite garantizar la seguridad de la información transmitida (asegurar la integridad de la misma – Firma digital) y recibida (protección contra virus que pueden infectar las PCs a través de este medio).
- Asegurar la adecuada manipulación y cuidado realizado a los medios removibles de la institución. Ayudando esto a la confidencialidad de los datos contenidos en los medios.
- Proveer a los administradores de los sistemas de una información completa de los registros del sistema.

#### 4.5.13.3 Análisis Económico

En base a los riesgos definidos, identificamos y estimamos el valor de cada uno de los activos que pueden verse afectados por los mismos, para lo cual, consideramos el tiempo y los recursos que son necesarios invertir para recuperar o recrear el activo en cuestión:

| Amenazas                                                                | Activos                | Tiempo Estimado de Recuperación                                                                                         | Recursos                        | Tiempo Total | Salario por Hora <sup>115</sup> | Valor del Activo                        |
|-------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------|--------------|---------------------------------|-----------------------------------------|
| Daño o alteración de la información. debido a cambios mal implementados | Activos de Información | 42 horas <sup>116</sup>                                                                                                 | 1 persona (Informática)         | 42 horas     | \$133,00                        | \$12.768,00                             |
|                                                                         |                        | 18 horas <sup>117</sup>                                                                                                 | 3 personas (sector en cuestión) | 54 horas     | \$133,00                        |                                         |
| Fuga de información                                                     | Activos de Información | **En caso de Fuga de Información, pueden existir costos legales, y puede ser necesario indemnizar a la persona afectada | --                              | --           | \$133,00                        | \$605.897,5 <sup>2</sup> <sup>118</sup> |
| Ataque de código malicioso a la infraestructura tecnológica             | Activos de Información | 70 horas <sup>119</sup>                                                                                                 | 1 persona (Informática)         | 70 horas     | \$133,00                        | \$9.310,00                              |
|                                                                         | Activos de Software    | 560 horas <sup>120</sup>                                                                                                | 1 persona (Informática)         | 560 horas    | \$133,00                        | \$74.480,00                             |
| Riesgo de phishing y spam                                               | Activos de Información | 12 horas <sup>121</sup>                                                                                                 | 1 persona (Informática)         | 12 horas     | \$133,00                        | \$1.596,00                              |
|                                                                         | Activos de Software    | 4 horas <sup>122</sup>                                                                                                  | 1 persona (Informática)         | 4 horas      | \$133,00                        | \$532,00                                |

<sup>115</sup> Se utilizó un Salario mensual de \$16000 con 30 hs semanales de trabajo.

<sup>116</sup> En caso que un cambio mal implementado afecte al funcionamiento del sistema, se estima un tiempo necesario para volver atrás los cambios implementados, en encontrar el error, corregirlo y realizar nuevamente el despliegue.

<sup>117</sup> Tiempo estimado que tarda una persona tarda en volcar su trabajo (de 7 días perdidos por la corrección de errores en los cambios) nuevamente al sistema.

<sup>118</sup> Se estima a partir de la fórmula de Vuotto, con  $n=23,5$  y  $a=48750$  (salario mensual de \$15.000 y un porcentaje de incapacidad de 0,25). Daño por la información filtrada.

<sup>119</sup> En caso de la existencia de un virus complejo, es posible que la información de las computadoras se dañe. Por lo cual se estima un tiempo necesario para pasar por 140 computadoras, determinar daño sobre la información, y en caso de ser necesario recuperar la misma (de los backups, discos particionados, etc.).  $30 \text{ min} * 140 = 4200 \text{ min} = 70 \text{ hs}$ .

<sup>120</sup> En caso de la existencia de un virus complejo, es posible que el SO de las computadoras este dañado. Por lo cual se estima un tiempo necesario para pasar por 140 computadoras, y recuperar/formatear el equipo.  $4 \text{ horas} * 140 = 560 \text{ horas}$ .

<sup>121</sup> Tiempo Estimado en recuperar la información eliminada por un virus. (Una computadora, se requiere utilizar programas para recuperar información del disco)

<sup>122</sup> Tiempo estimado en eliminar el virus y en formatear y recuperar el pc.

|                                         |                        |                          |                             |             |          |                |
|-----------------------------------------|------------------------|--------------------------|-----------------------------|-------------|----------|----------------|
| Perdida de total de Información digital | Activos de Información | 480 horas <sup>123</sup> | 140 empleados (como mínimo) | 67200 horas | \$133,00 | \$8.937.600,00 |
|-----------------------------------------|------------------------|--------------------------|-----------------------------|-------------|----------|----------------|

Tabla 4.5-36

A continuación, calculamos la Expectativa de Pérdida Individual para cada uno de los activos identificados anteriormente:

| Activo                 | Amenaza                                                                 | Valor del Activo | EF (Factor de Exposición) | SLE (Expectativa de Pérdida Individual) |
|------------------------|-------------------------------------------------------------------------|------------------|---------------------------|-----------------------------------------|
| Activos de Información | Daño o alteración de la información. debido a cambios mal implementados | \$12.768,00      | 0,5                       | \$6.384,00                              |
| Activos de Información | Fuga de información                                                     | \$605.897,52     | 0,65                      | \$393.833,39                            |
| Activos de Información | Ataque de código malicioso a la infraestructura tecnológica             | \$9.310,00       | 0,5                       | \$4.655,00                              |
| Activos de Software    |                                                                         | \$74.480,00      | 0,5                       | \$37.240,00                             |
| Activos de Información | Riesgo de phishing y spam                                               | \$1.596,00       | 0,5                       | \$798,00                                |
| Activos de Software    |                                                                         | \$532,00         | 0,5                       | \$266,00                                |
| Activos de Información | Perdida de total de Información digital                                 | \$8.937.600,00   | 0,6                       | \$5.362.560,00                          |

Tabla 4.5-37

Con el propósito de calcular la Expectativa de Pérdida Anual (ALE), se realizó una estimación de la Tasa de Ocurrencia Anualizada (ARO), debido a la inexistencia de datos históricos de incidentes de seguridad de la información dentro de la organización, y se obtuvieron los siguientes valores:

| Activo                 | Amenaza                                                                 | SLE (Expectativa de Pérdida Individual) | ARO (Tasa de Ocurrencia Anualizada) | ALE (Expectativa de Pérdida Anual) |
|------------------------|-------------------------------------------------------------------------|-----------------------------------------|-------------------------------------|------------------------------------|
| Activos de Información | Daño o alteración de la información. debido a cambios mal implementados | \$6.384,00                              | 0,2                                 | \$1.276,80                         |

<sup>123</sup> Se estima que: para 6 horas laborales por día, se tienen 1440 horas trabajadas en 1 año. De las cuales 3 horas estimadas por día para cargar información al sistema = 480 anuales de carga de información.

|                        |                                                             |                |      |                     |
|------------------------|-------------------------------------------------------------|----------------|------|---------------------|
| Activos de Información | Fuga de información                                         | \$393.833,39   | 0,5  | \$196.916,69        |
| Activos de Información | Ataque de código malicioso a la infraestructura tecnológica | \$4.655,00     | 0,2  | \$931,00            |
| Activos de Software    |                                                             | \$37.240,00    | 0,2  | \$7.448,00          |
| Activos de Información | Riesgo de phishing y spam                                   | \$798,00       | 0,6  | \$478,80            |
| Activos de Software    |                                                             | \$266,00       | 0,6  | \$159,60            |
| Activos de Información | Perdida de total de Información digital                     | \$5.362.560,00 | 0,05 | \$268.128,00        |
| <b>Total</b>           |                                                             |                |      | <b>\$475.338,89</b> |

Tabla 4.5-38

Como podemos ver, el total obtenido en la tabla anterior constituye la pérdida anual de la organización por no llevar adelante una adecuada gestión de comunicaciones y operaciones.

## 4.6 Control de Accesos

### 4.6.1 Requerimientos para el control de accesos

*“Objetivo: Controlar el acceso a la información.*

*Se recomienda que se controle el acceso a la información, a las instalaciones de procesamiento de la información y a los procesos de negocios, sobre la base de los requerimientos de seguridad y de los negocios.*

*Se recomienda que las reglas de control de acceso tengan en cuenta las políticas de autorización y de difusión de la información.”<sup>124</sup>*

#### 4.6.1.1 Política de control de accesos

##### **Control**

*“Se recomienda que se establezca, documente y revise una política de control de accesos basada en los requerimientos de acceso de seguridad y del negocio”<sup>125</sup>*

##### **Relevamiento**

Con el fin de corroborar el cumplimiento de los lineamientos propuestos por el control bajo estudio, se realizaron las siguientes actividades:

<sup>124</sup> IRAM-ISO/IEC 27002:2008

<sup>125</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

- Con el propósito de analizar el control de acceso a la información del sistema, se realizó una entrevista con el jefe del sector de sistemas informáticos, ya que, es responsabilidad del sector controlar el acceso a la información del sistema. Durante la entrevista se realizaron las siguientes preguntas, en base a lo establecido en el control “Política de control de accesos” de la norma IRAM-ISO/IEC 27002:2008:

- ¿Existe una política de control de accesos en la institución?
- ¿De qué manera se controla el acceso a la información del sistema?

- Con el fin de analizar el control de acceso a la información plasmada en papel, se realizó una entrevista a cada jefe de sector/programa de las áreas bajo estudio.

Durante la entrevista se realizaron las siguientes preguntas, en base a lo establecido en el control “Política de control de accesos” de la norma IRAM-ISO/IEC 27002:2008:

- ¿De qué manera se controla el acceso a la información (en papel) manejada por el sector?

- Análisis de la documentación que contiene la misión, visión y funciones de los sectores/programas de la institución.

En base a la información obtenida durante las entrevistas, realizadas el día 15/03/2016, y del análisis de la documentación correspondiente, se procedió a completar el siguiente checklist

| Política de control de acceso                                                                              | Sí | No |
|------------------------------------------------------------------------------------------------------------|----|----|
| ¿Existe en la organización una política de control de acceso?                                              |    | X  |
| Se tiene en cuenta en la política (o de manera informal) los siguientes puntos:                            |    | X  |
| Requerimientos de seguridad de las aplicaciones                                                            |    | X  |
| Identificación de toda la información relacionada con las aplicaciones y el riesgos de la misma            |    | X  |
| Políticas de divulgación y autorización de información                                                     |    | X  |
| Legislación aplicable                                                                                      |    | X  |
| Perfiles de acceso de usuarios normales                                                                    |    | X  |
| Gestión de los derechos de acceso en un ambiente distribuido y de red (tipos de conexiones, acceso remoto) |    | X  |
| Separación de los roles de control de acceso                                                               |    | X  |
| Requerimientos de autorización formal de los pedidos de acceso                                             |    | X  |
| Requerimientos para las revisión periódica de los controles de acceso                                      |    | X  |
| Remoción de los derechos de acceso                                                                         |    | X  |

Tabla 4.6-1

Como puede observarse en el anterior checklist, no existe en la organización una política de control de acceso, razón por la cual no se cumple con ninguno de los puntos establecidos por el presente control.

Es necesario aclarar que actualmente el jefe de cada sector/programa en colaboración con la gerencia (responsables de la información generada por cada sector/programa) otorga a las personas bajo su cargo la autorización para la manipulación de la información generada por cada sector/programa, y es responsabilidad del jefe de sector/programa el cuidado de dicha información. Por otro lado, el acceso al sistema ERP de la institución es otorgado por el sector de sistemas informáticos. Este sector se encarga de verificar que el usuario posee autorización requerida (solo consultar la información necesaria) para acceder al sistema ERP. Sin embargo, es necesario destacar que el acceso otorgado al personal de la institución, tanto a la documentación como al sistema de información, se realiza informalmente.

#### 4.6.1.1.1 Cambios recomendados

Debido a la inexistencia de una política de control de acceso en la institución, se recomienda la elaboración y documentación de la misma. Es necesario que esta sea elaborada por el responsable de seguridad de la información en colaboración con el jefe del sector de sistemas informáticos. Esta política debe ser evaluada y aprobada por el comité de seguridad de la información y por la gerencia del hospital.

La Política de control de acceso debe respetar la siguiente estructura:

1. Objetivo
2. Alcance
3. Puntos específicos

Debe tener en cuenta los siguientes aspectos:

- Tener consistencia con las políticas existentes. (Acuerdo de confidencialidad, política de clasificación de la información, etc.)
- Establecer requerimientos de seguridad de las aplicaciones (Establecer aspectos claves a tener en cuenta para la protección de las aplicaciones). La identificación de toda la información relacionada con las aplicaciones es necesaria para establecer los requerimientos.
- Establecer los roles y responsabilidades.
- Establecer las reglas para la gestión de accesos de los usuarios (Procedimiento de alta y baja de usuarios, gestión de los privilegios, gestión de contraseñas)
- Considerar la remoción de los derechos de acceso (ver 4.4.3.4(Remoción de Derechos de Acceso))
- Aclarar las responsabilidades de los usuarios (reglas para el uso de contraseñas, reglas para el manejo de los equipos de procesamiento de la información, reglas para el manejo de la documentación).
- Establecer las pautas para la adecuada gestión de las redes.
- Establecer las pautas para la adecuada gestión del acceso a los sistemas operativos.

#### 4.6.2 Gestión de acceso de usuarios

*“Objetivo: Asegurar el acceso a los usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información.*

*Se recomienda que se encuentren establecidos procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.*

*Se recomienda que los procedimientos cubran todas las etapas del ciclo de vida del acceso de usuario, desde el registro inicial de nuevos usuarios hasta la eliminación final de los registros de los usuarios quienes ya no requieren acceso a los sistemas y servicios. Se recomienda especial atención, cuando corresponda, a la necesidad de controlar la asignación de derechos de acceso privilegiados, que permiten a los usuarios sustituir los controles del sistema.”<sup>126</sup>*

#### 4.6.2.1 Registro de usuarios

##### **Control**

*“Se recomienda que exista un procedimiento formal de registro de alta y baja de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información”<sup>127</sup>*

##### **Relevamiento**

Con el fin de corroborar el cumplimiento de los lineamientos propuestos por el control bajo estudio, se realizaron las siguientes actividades:

- Entrevista al jefe del sector de sistemas informáticos, debido a que este sector se encarga de realizar el registro de todos los usuarios del sistema.  
En base a lo establecido en el control “Registro de usuarios” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:
  - ¿Existe un procedimiento formal de registro de alta y baja de usuarios?
- Observación: Se solicitó a un administrador del sistema (jefe del sector de informática) la creación de un usuario de prueba, con el propósito de visualizar la forma mediante la cual los permisos de acceso son creados y otorgados al usuario que lo requiere. Durante la creación del usuario, se interrogó al administrador sobre:
  - ¿El usuario creado es único?
  - ¿Se solicita autorización para la creación?
  - ¿Se verifica que los permisos otorgados sean acordes al puesto de trabajo (solo acceder a los datos que son necesarios)?
  - ¿Se otorgan al usuario declaración en la cuales se establecen sus derechos de acceso?
  - ¿Siempre es presencial la entrega de usuarios? ¿Se realizan excepciones para entrar los permisos (sin verificar autorización o identidad)?
  - ¿Se eliminan los usuarios (por desvincularon o cambio de puesto)?

Conforme a los datos obtenidos durante la entrevista realizada al jefe del sector de sistemas informáticos, realizada el día 15/03/2016, y a la simulación de creación de usuario, se completó el siguiente Checklist:

---

<sup>126</sup> IRAM-ISO/IEC 27002:2008

<sup>127</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

| Registro de usuario                                                                                    | Sí | No |
|--------------------------------------------------------------------------------------------------------|----|----|
| ¿Existe un procedimiento formal de registro de alta y baja de usuarios?                                |    | X  |
| Se tiene en cuenta en el procedimiento ( o de manera informal) los siguientes puntos:                  |    |    |
| Utilización de identificaciones únicas de usuarios                                                     | X  |    |
| Verificación de que el usuario tiene autorización del dueño del sistema para el uso del mismo          | X  |    |
| Verificación de que el nivel de acceso otorgado es el adecuado (cumple con la seguridad y la política) |    | X  |
| Entrega a los usuarios una declaración escrita de sus derechos de acceso                               |    | X  |
| Firma del usuario de la declaración de sus derechos de acceso                                          |    | X  |
| Verificación de que no se otorguen los permisos de acceso hasta después de completado el procedimiento | X  |    |
| Mantenimiento de un registro formal de todas las personas registradas para el uso del servicio         | X  |    |
| Remoción de los derechos de acceso en caso de cambio de puesto                                         | X  |    |
| Remoción de los derechos de acceso en caso de desvinculación                                           |    | X  |
| Verificación periódica del registro de usuarios (usuarios redundantes, eliminación, bloqueo)           |    | X  |

Tabla 4.6-2

Como es posible apreciar en el anterior checklist, el registro de alta y baja de los usuarios no se realiza por medio de un procedimiento formal, y es por esto que no se cumplimenta con el primer punto del checklist.

A pesar de la inexistencia de un procedimiento formal, puede observarse en el checklist que ciertos aspectos si se cumplen. Actualmente el sector de sistemas informáticos es el encargado de otorgar los permisos de acceso al sistema de la institución. Para obtener dichos permisos, el usuario, en primera instancia, solicita la autorización a la persona responsable del sector en el cual se desempeña (jefe de sector/programa), luego de esto, se dirige al sector de sistemas informáticos en donde le son solicitados sus datos personales (nombre completo, DNI, sector y otros datos según sea necesario) a fin de crear un usuario único (se verifica que el nombre de usuario no sea repetido) para hacer uso del sistema. Una vez creado el usuario se otorgan los permisos necesarios para esa cuenta y se verifican los mismos. El registro de todos los usuarios y sus respectivos permisos es llevado por el sistema (el sistema vincula el nombre de usuario con los datos dela persona). Por último, es necesario aclarar que el sector de sistema informático, únicamente en caso de cambio de puesto, realiza la remoción/cambio de los derechos de acceso. Debido a lo explicado previamente, consideramos que ciertos puntos se cumplen, y es por esto que concluimos que el actual control se cumple parcialmente en la institución.

*Yustman, Mauricio Ezequiel*

*Pérez Osán, Fernando Javier*

*Página 231*

Vale la pena aclarar que en la institución se otorga acceso al servicio de red WIFI mediante un procedimiento formal (*“proceso para la autorización de equipos personales”*) previamente detallado en 4.2.1.4(Procedimiento de Autorización para instalaciones de procesamiento de información). Consideramos que este procedimiento cumple con la mayoría de los puntos requeridos por el presente control, por la tanto no son necesarias modificaciones al mismo.

#### 4.6.2.1.1 Cambios recomendados

Debido a la inexistencia de un proceso formal para el registro de alta y baja de usuarios de los servicios y sistemas de información, y a pesar de la existencia de ciertas medidas informales tomadas para esto, consideramos que para cumplimentar con lo establecido por el presente control es necesario adoptar el siguiente procedimiento:

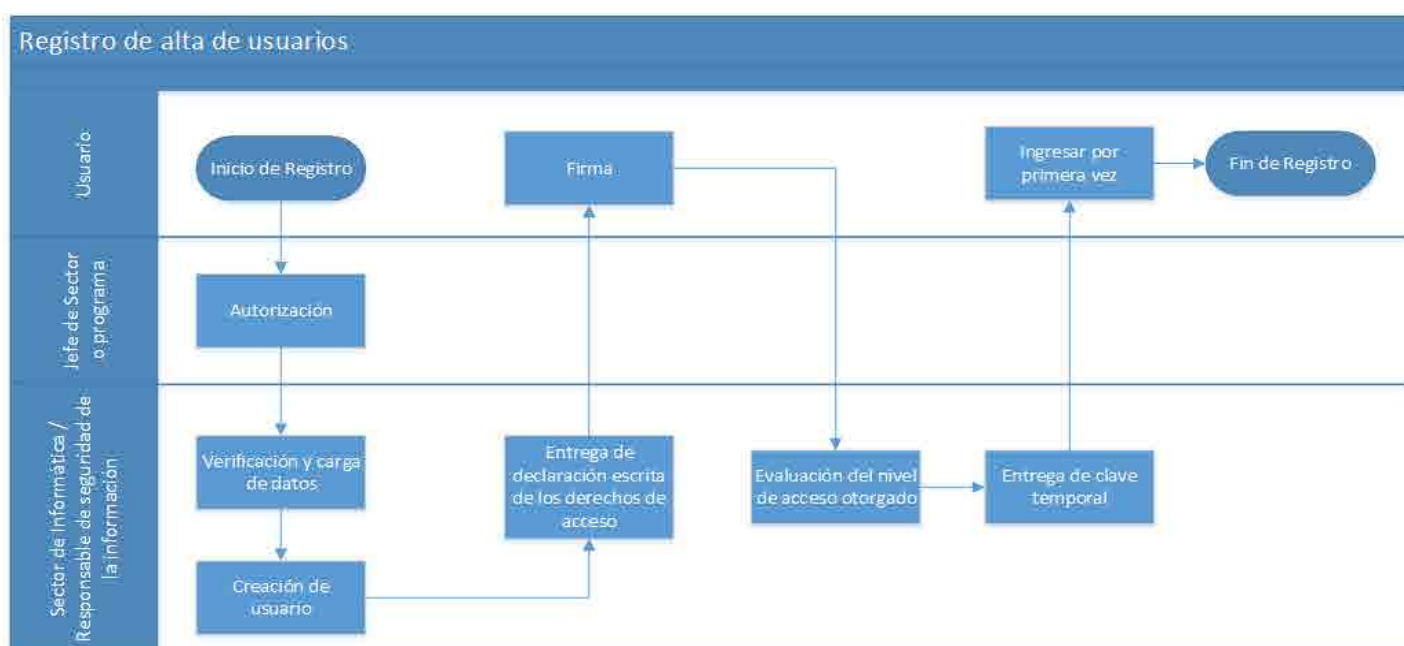


Ilustración 4.6-1

- I. Inicio de registro: La persona solicita obtener acceso al sistema. Para ello esta debe solicitar, en primera instancia, autorización al jefe de programa/sector (debido a que este es el propietario de los datos generados en el sector/programa) en donde trabaja.
- II. Autorización: el jefe de programa/sector autoriza al personal en cuestión para obtener acceso al sistema. Luego de esto, solicita al sector de sistemas informáticos a través del correo institucional (es importante destacar que este correo es firmado digitalmente por el jefe del sector, para así corroborar la identidad del mismo y la validez de la autorización) la entrega de los derechos de acceso al usuario en cuestión.
- III. El usuario solicitante, debe dirigirse al sector de sistemas informáticos a fin de pedir la creación de un usuario que le permita acceder al sistema y a los diferentes servicios que posee la institución.
- IV. Verificación y carga de datos: El administrador del sistema (persona del sector con los privilegios adecuados para la creación de usuarios) corrobora la existencia del correo electrónico en el cual se solicita, por parte del jefe del sector, la entrega de los derechos de acceso al usuario. Posteriormente, se solicitan los datos personales de esta (nombre

completo, DNI, sector y otros datos según sea necesario). Estos datos son cargados en el sistema.

- V. Creación de usuario: El administrador del sistema crea un usuario para el acceso al sistema (basándose en los datos otorgados por la persona solicitante) y verifica que este sea único. Además, en base a los datos del usuario y las necesidades de uso de los servicios informáticos, es creado el correo institucional del usuario en cuestión y le son otorgadas sus credenciales de acceso al sistema operativo de las estaciones de trabajo.
- VI. Entrega de declaración escrita de los derechos de acceso: El responsable de seguridad de la información debe entregar un documento a la persona solicitante en donde detallen los siguientes aspectos:
- Importancia de conservar en secreto las credenciales de acceso al sistema (usuario y contraseña) y a los servicios informáticos
  - Importancia de realizar solamente las tareas para las que fueron autorizados y de no hacer un uso mal intencionado del sistema y los recursos informáticos a los cuales tiene acceso.
  - Aclarar que el usuario solo debe acceder a los módulos/datos que tiene permitido. Se debe aclarar cuáles son estos módulos/datos. Es importante comunicar al usuario que, en caso de acceder a otros datos no permitidos, esto puede incurrir en sanciones disciplinarias debido al mal uso del sistema.
  - Aclarar que toda actividad realizada por una cuenta de usuario es registrada por el sistema.
  - Importancia de conservar la confidencialidad de los datos accedidos a través del sistema (ver 4.2.1.5.1(Acuerdo de confidencialidad)).
  - Dejar en claro los puntos detallados en Uso aceptable de los activos ( ver 4.3.1.3)

Este documento servirá de remito de entrega de las credenciales de acceso al sistema

- VII. Firma: la persona solicitante firma el documento, dejando en claro así que comprende las condiciones de acceso. Este documento es firmado por duplicado, quedando una copia en manos del usuario y otra en el sector de sistemas informáticos.
- VIII. Verificación del nivel de acceso: el administrador del sistema en colaboración con el responsable de seguridad de la información, realizan la evaluación del nivel de acceso necesario a otorgar para el usuario creado (de acuerdo a las necesidades y responsabilidades del usuario. Se debe respetar la política de acceso). Una vez evaluado esto se otorgan los permisos de acceso para el usuario en cuestión. (permisos de acceso al sistema, permisos de acceso a las estaciones de trabajo/S.O)
- IX. Entrega de clave temporal: El administrador del sistema entrega a la persona solicitante las credenciales de acceso al sistema y a las estaciones de trabajo (Usuario y contraseña). Es importante destacar que es necesario el uso de claves temporales (ver 4.6.2.3.1(Gestión de contraseñas de usuario)). Además de la entrega de las credenciales de acceso antes mencionadas, debe hacerse entrega de una guía de buenas prácticas para la selección y uso de contraseñas. (ver 4.6.3.1.1(Uso de contraseñas)). Es importante considerar que la entrega de estas credenciales no debe realizarse por medios electrónicos o ser transmitidas a través de papel. Son otorgadas también las credenciales de acceso al correo institucional.
- X. Ingresa por primera vez: La persona solicitante accede al sistema/ Estación de trabajo por primera vez con las credenciales otorgadas. Es necesario destacar que, debido a la

entrega de una clave temporal, el usuario en su primer acceso deberá cambiar la contraseña temporal por una contraseña propia (El sistema/controlador de dominio debe obligar al usuario a realizar esta acción)

Es necesario aclarar que el sistema debe llevar un registro con todos los usuarios creados para acceder al mismo. Así mismo, debe llevarse un registro asociado a cada usuario en donde se detallen los derechos de acceso del mismo. Es importante que se realicen periódicamente revisiones de dichos registros, con el objetivo de garantizar que los mismos son completos y actualizados.

Por último, para la remoción de los derechos de acceso ya sea por desvinculación o cambio de puesto, debe adoptarse la solución detallada en **4.4.3.4**(Remoción de derechos de acceso). Es necesario aclarar la importancia de realizar la verificación de identidad en caso de cambio de puesto, para así evitar modificar derechos de accesos de manera errónea.

#### 4.6.2.2 Gestión de privilegios

##### **Control**

*“Se recomienda que la asignación y uso de los privilegios este restringido y controlado”<sup>128</sup>*

##### **Relevamiento**

Con el fin de corroborar el cumplimiento de los lineamientos propuestos por el control bajo estudio, se realizaron las siguientes actividades:

- Entrevista al Jefe del Sector de Sistemas Informáticos, dado que, es este sector el encargado de gestionar la asignación de privilegios del sistema.  
De acuerdo a lo establecido en el control “*Gestión de privilegios*” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:
  - ¿Existe un procedimiento formal para la asignación y autorización de privilegios de acceso?
  - Los administradores del sistema ¿Cuántos son?
  - Los privilegios de administración ¿Cómo son otorgados?
- Observación: Se solicitó al administrados del sistema, visualizar (hacer una demostración) la manera mediante la cual los permisos/derechos de acceso son otorgados para un usuario en particular del sistema.

Conforme a los datos obtenidos durante la entrevista realizada el día 15/03/2016, y a la observación realizada, se completó el siguiente Checklist:

| Gestión de privilegios                                                                      | Sí | No |
|---------------------------------------------------------------------------------------------|----|----|
| ¿Existe un procedimiento formal para la asignación y autorización de privilegios de acceso? |    | X  |
| Se tiene en cuenta en el procedimiento ( o de manera informal) los siguientes puntos:       |    |    |

<sup>128</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

|                                                                                                            |   |   |
|------------------------------------------------------------------------------------------------------------|---|---|
| Identificación de los privilegios de acceso                                                                | X |   |
| Asignación de los privilegios a los individuos sobre las bases de necesidad de uso                         | X |   |
| Registro de los privilegios asignados                                                                      | X |   |
| Promover el desarrollo y uso de rutinas para evitar la necesidad de otorgar privilegios de usuario         |   | X |
| Promover el desarrollo y uso de programas que eviten la necesidad de ser ejecutadas con privilegios        |   | X |
| Los privilegios de administración estén asignados con identificadores de usuarios diferentes a lo normales | X |   |

Tabla 4.6-3

Como es posible apreciar en el checklist, no existe un procedimiento formal para otorgar privilegios de acceso, es por esto que el primer punto del anterior checklist no se cumplimenta en la organización. Sin embargo, informalmente se realiza una revisión de los derechos de acceso necesarios (de acuerdo a sus necesidades de uso) para un usuario cuando este es creado y otorgado.

Por otro lado, los privilegios de administración del sistema (sistema y base de datos) únicamente son otorgados al personal del sector de sistemas informáticos (por política interna del sector a ningún otro usuario del sistema se les asignan privilegios de acceso), estos privilegios tienen una identificación diferente a los usuarios normales y se lleva un registro (en el sistema) que detalla los privilegios que son otorgados y el usuario asociado.

#### 4.6.2.2.1 Cambios recomendados

Debido a la inexistencia de un procedimiento formal para otorgar privilegios de acceso al sistema, recomendamos adoptar el procedimiento detallado en **4.6.2.1.1**(Registro de usuarios). En dicho procedimiento puede observarse que se realiza la identificación de los permisos de acceso necesarios para un usuario, así como también, la autorización necesaria para esto (documento de autorización). También puede observarse que se realiza una evaluación de los permisos de acceso otorgados (en base a las necesidades de uso y de acuerdo a las políticas) y se lleva un registro de los permisos otorgados.

Por último, debido a que el sistema es administrado solamente por el personal de sistemas informáticos (particularmente dos personas), recomendamos que los privilegios de administración otorgados a estas personas sean revisados por el comité de seguridad y sea este comité el encargado de realizar revisiones periódicas sobre estas cuentas de administrador.

#### 4.6.2.3 Gestión de contraseñas de usuario

##### **Control**

*“Se recomienda que la asignación de contraseñas se controle mediante un proceso formal de gestión”<sup>129</sup>*

<sup>129</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

### **Relevamiento**

Con el fin de corroborar el cumplimiento de los lineamientos propuestos por el control bajo estudio, se realizaron las siguientes actividades:

- Entrevista al Jefe del Sector de Sistemas Informáticos, ya que, es este sector en encargado de la gestión de los usuarios del sistema.  
 Teniendo en cuenta lo establecido en el control “*Gestión de contraseñas de usuario*” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:
  - ¿Existe un procedimiento formal para la gestión contraseñas de usuarios?
  - ¿Qué aspectos se tienen en cuenta para la gestión de las contraseñas?
- Observación: Se solicitó a un administrador del sistema (jefe del sector de informática) la creación de un usuario de prueba, con el propósito de visualizar la forma mediante la cual son entregadas las credenciales de acceso (usuario y contraseña)

Conforme a los datos obtenidos durante la entrevista realizada al jefe del sector de sistemas informáticos, realizada el día 15/03/2016, y a la observación realizada, se completó el siguiente Checklist:

| Gestión de contraseñas de usuario                                                                                                    | Sí | No |
|--------------------------------------------------------------------------------------------------------------------------------------|----|----|
| ¿Existe un procedimiento formal para la gestión de contraseñas?                                                                      |    | X  |
| Se tiene en cuenta en el procedimiento ( o de manera informal) los siguientes puntos:                                                |    |    |
| Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener en secreto las contraseñas                    |    | X  |
| Los usuarios manejen sus propias contraseñas                                                                                         | X  |    |
| Otorgar contraseña temporal                                                                                                          |    | X  |
| Establecer un procedimiento para verificar la identidad de un usuario antes de proveerle una contraseña nueva (cambio de contraseña) | X  |    |
| Las contraseñas temporales se otorguen de manera segura (no mail, no terceras partes)                                                |    | X  |
| Las contraseñas temporales sean únicas y no adivinables                                                                              |    | X  |
| Poseer un remito de recepción de contraseña                                                                                          |    | X  |
| Las contraseñas deben almacenarse en sistemas informáticos de forma protegida                                                        | X  |    |
| Cambiar la contraseña por defecto luego de la instalación.                                                                           | X  |    |

Tabla 4.6-4

Como detalla el checklist, no existe un procedimiento formal para la gestión de contraseñas de usuario. Actualmente los usuarios que solicitan una contraseña de acceso al sistema ERP, deben presentarse personalmente en el sector de sistemas informáticos solicitando

la misma, es en ese sector donde se corrobora la autorización correspondiente y se solicitan los datos de la persona; posteriormente, el usuario registra en el sistema su contraseña (no se otorgan contraseñas temporales). En caso de necesitar un cambio de contraseña, los usuarios deben presentarse personalmente al sector de sistemas informáticos para cambiar la misma. Los datos de los usuarios y sus contraseñas son almacenados en el sistema.

Por otro lado, todo el equipamiento (servidores, dispositivos de red) es configurado por primera vez por el sector de sistemas informáticos, en donde las contraseñas por defecto otorgadas por el fabricante son cambiadas apropiadamente. El sector lleva un registro de estas contraseñas.

En cuanto a las contraseñas de acceso al servicio de red WIFI, las personas también deben presentarse personalmente en el sector de sistemas informáticos solicitando el permiso de acceso. Tal como lo detalla el procedimiento **4.2.1.4**(Proceso para la autorización de equipos personales), los usuarios deben firmar las condiciones de uso. En estas condiciones de uso (ver **7.4**) se especifica que los usuarios se comprometen a guardar la confidencialidad de sus contraseñas y no deben compartirlas. Posteriormente firman las condiciones de uso y el usuario registra su contraseña. El usuario, en caso de necesitar un cambio de contraseña, debe presentarse personalmente en el sector de sistemas informáticos.

Por todo lo explicado previamente y considerando que no se otorgan contraseñas temporales, concluimos que el presente control se cumple parcialmente dentro de la institución.

#### 4.6.2.3.1 Cambios recomendados

Debido a que en la institución no se emplean contraseñas temporales y a la inexistencia de un procedimiento formal para la gestión de las mismas, recomendamos adoptar el procedimiento detallado en **4.6.2.1.1**(Registro de usuarios). Tal como se detalla en dicho procedimiento, al momento de entregar las credenciales de acceso al sistema, deben otorgarse contraseñas temporales. Es por esto que consideramos necesario que el sistema sea modificado de manera tal que, para el registro de usuarios, se emplee el uso de contraseñas temporales. Para el uso de contraseñas temporales deben considerarse los siguientes aspectos:

- La importancia de verificar la identidad de la persona/usuario al momento de solicitar un cambio de contraseña. Es recomendable que en estos casos se realice un “blanqueo de contraseña”, para que de esta manera cuando el usuario ingrese al sistema, le sea solicitado ingresar una clave personal nuevamente (igual que cuando se realiza el ingreso por primera vez (ver **4.6.2.1.1**(procedimiento))
- Entregar las contraseñas temporales de manera segura. (No realizar la entrega mediante mail (o algún otro medio electrónico) o escritas)
- Generar claves temporales únicas para cada usuario.

Es importante aclarar que las contraseñas generadas por los usuarios deben ser almacenadas en el sistema de manera segura (es recomendable usar una técnica de cifrado)

Es recomendable que el administrador del sistema considere las siguientes pautas para llevar a cabo una gestión adecuada y seguridad de las contraseñas de usuario:

- NO permitir el uso de cuentas de usuario sin contraseña.
- Asegurarse de cambiar las contraseñas por defecto del sistema (root, system, guest, demo, etc.).

- Considerar implementar modificaciones al sistema para una gestión más segura de contraseñas tales como:
  - ✓ Número limitado de intentos fallidos de acceso
  - ✓ Longitud mínima de contraseña requerida
  - ✓ Formato determinado de contraseña (Mayúscula, Minúsculas, caracteres especiales, caracteres numéricos)
  - ✓ Envejecimiento de contraseña (obligar a cambiar la contraseña después de transcurrido cierto tiempo y asegurarse que la nueva contraseña no sea igual a la anterior)

#### 4.6.2.4 Revisión de los derechos de acceso

##### **Control**

*“Se recomienda que la alta dirección revise los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal”<sup>130</sup>*

##### **Relevamiento**

Con el fin de corroborar el cumplimiento del presente control en el hospital se realizó una entrevista con el jefe del sector de sistemas informáticos, ya que, es responsabilidad del sector la gestión de los derechos de acceso otorgados a los usuarios del sistema.

Durante la entrevista se realizaron las siguientes preguntas, en base a lo establecido en el control “Revisión de los derechos de acceso” de la norma IRAM-ISO/IEC 27002:2008:

- ¿La alta dirección realiza revisiones de los derechos de acceso otorgados?
- ¿Con que frecuencia se realizan estas revisiones y que proceso es utilizado para ello?
- ¿Qué puntos/directrices se consideran para realizar las revisiones?

En base a la información obtenida durante la entrevista, realizada el día 15/03/2016, se procedió a completar el siguiente checklist

| Revisión de los derechos de acceso                                                                           | Sí | No |
|--------------------------------------------------------------------------------------------------------------|----|----|
| ¿La alta dirección revisa los derechos de acceso a intervalos regulares utilizando un proceso formal?        |    | X  |
| Las revisiones de los derechos de acceso tienen en cuenta las siguientes directrices (formal/informalmente): |    |    |
| Se realiza la revisión a intervalos regulares de tiempo (cada 6 meses, después de un cambio, etc.)           |    | X  |
| Revisión y reasignación de derechos de acceso ante un traslado                                               | X  |    |
| Revisión a intervalos más frecuentes de los privilegios de acceso (controlar la asignación no autorizada)    |    | X  |
| Registro de los cambios en cuentas privilegiadas                                                             |    | X  |

Tabla 4.6-5

<sup>130</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

Como puede observarse en el anterior checklist, la alta dirección del hospital no realiza revisiones periódicas de los derechos de acceso otorgados, es por esto que consideramos que el presente control no cumple con la mayoría de los puntos del presente control.

Es importante destacar que el sector de sistemas informáticos es el encargado de otorgar (con previa autorización del propietario de los datos (gerencia/jefe de sector/programa)) y gestionar los derechos de acceso. Ante un cambio de puesto, el sector de sistemas informáticos realiza, en caso de ser necesario, la revisión y reasignación de los derechos de acceso al sistema (esta reasignación es solicitada por el usuario o el jefe del sector/programa involucrado).

#### 4.6.2.4.1 Cambios recomendados

Debido a la inexistencia de revisiones periódicas de los derechos de acceso, consideramos que es necesario, para cumplimentar con los puntos propuesto por el presente control, realizar estas revisiones. Recomendamos que las mismas sean realizadas por el comité de seguridad y que se consideren las siguientes directrices:

- Verificar que los permisos/privilegios otorgados son los adecuados. (son acordes para las tareas que debe realizar el usuario y acordes a las políticas de la institución)
- Realizar las revisiones a intervalos regulares de tiempo. Durante las mismas deben evaluarse todos los cambios realizados en los permisos de acceso (cambios producidos por desvinculación o cambio de puesto) y llevarse un registro de los mismos.
- Realizar revisiones más regulares para aquellos usuarios con permisos de acceso especiales (privilegios de administración). Durante estas revisiones debe prestarse especial atención en la autorización de las mismas y en los privilegios otorgados (debe verificarse que los privilegios otorgados están autorizados y que no existen privilegios otorgados sin autorización).
- Llevar un registro de todos los cambios en las cuentas con privilegios de administración.

#### 4.6.3 Responsabilidades del usuario

*“Objetivo: prevenir el acceso de usuarios no autorizados, de modo que se comprometa o sustraiga la información o las instalaciones de procesamiento de la información.*

*La cooperación de los usuarios autorizados es esencial para que la seguridad sea efectiva.*

*Se recomienda que se concientice a los usuarios de sus responsabilidades para el mantenimiento efectivo de controles de acceso, particularmente los relacionados con el uso de contraseñas y la seguridad del equipamiento del usuario.*

*Se recomienda que se implemente una política de mantener el escritorio y la pantalla limpios para reducir el riesgo del acceso no autorizado o daño a papeles, a los medios y a las instalaciones de procesamiento de la información.”<sup>131</sup>*

##### 4.6.3.1 Uso de contraseñas

#### **Control**

---

<sup>131</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

*“Se recomienda que se solicite a los usuarios que sigan las buenas prácticas de seguridad en la selección y uso de contraseñas”<sup>132</sup>*

### **Relevamiento**

Con el fin de corroborar el cumplimiento de los lineamientos propuestos por el control bajo estudio, se realizaron las siguientes actividades:

- Entrevista al jefe del sector de sistemas informáticos, debido a que es dicho sector el encargado de otorgar las contraseñas de acceso a los sistemas de información.  
En base a lo establecido en el control “*Uso de contraseñas*” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:
  - Al momento de entregar las contraseñas a los usuarios, ¿se les comunican buenas practica para la selección y uso de contraseñas?
  - ¿Qué recomendaciones se les da a los usuarios para la selección y uso de contraseñas?
- Observación: Se solicitó modificar la contraseña del usuario de prueba creado con el fin de corroborar el tipo de contraseña admitida por el sistema.

En base a la información obtenida durante la entrevista, realizada el día 15/03/2016, y a la observación, se procedió a completar el siguiente checklist

| Uso de contraseñas                                                                                                                      | Sí | No |
|-----------------------------------------------------------------------------------------------------------------------------------------|----|----|
| ¿A los usuarios se les comunican las buenas prácticas de seguridad en la selección y uso de contraseñas?                                |    | X  |
| Se comunica a los usuarios los siguientes puntos (formal/informalmente):                                                                |    |    |
| Mantener las contraseñas de manera confidencial                                                                                         | X  |    |
| Evitar mantener un registro inapropiado de contraseñas (papeles, en dispositivos móviles, software)                                     |    | X  |
| Cambiar las contraseñas ante la posibilidad de que un sistema o contraseña se encuentren comprometidos                                  |    | X  |
| Selección de contraseñas de calidad (fáciles de recordar, no basadas en datos fáciles de adivinar, no utilizar palabras de diccionario) |    | X  |
| Cambiar de contraseña a intervalos regulares                                                                                            |    | X  |
| No guardar contraseñas en procesos automatizados de ingreso                                                                             |    | X  |
| No usar una misma contraseña en diferentes sistemas                                                                                     |    | X  |

Tabla 4.6-6

Como es posible visualizar en el checklist, a los usuarios no se les comunican buenas prácticas para la selección y uso de contraseñas. El sector de sistemas informáticos deja a criterio del usuario la selección de la contraseña sin darle al mismo ninguna recomendación

<sup>132</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

para esto. Este sector únicamente comunica al usuario (informalmente) la importancia de mantener en secreto la contraseña utilizada para acceder a al sistema ERP de la institución. Por otro lado, cuando el sector otorga acceso a la red inalámbrica disponible en la institución, hace firmar al usuario unas condiciones de uso (ver 7.4) en la cual se detalla la importancia de mantener en secreto la contraseña utilizada por el usuario. Es por esto, que consideramos que únicamente se cumple con este punto (mantener en secreto las contraseñas) del presente control. Por lo tanto, concluimos que el presente no se cumplimenta dentro de la institución.

#### 4.6.3.1.1 Cambios recomendados

Para cumplimentar con el presente control, y considerando que no se les comunican a los usuarios buenas prácticas para la selección y uso de contraseña, recomendamos entregar al usuario el documento “Guía de buenas prácticas para la selección y uso de contraseñas” (ver 7.5). Este documento propuesto está sujeto a las modificaciones que se consideren necesarias y debe ser revisado por el comité de seguridad y aprobado por la gerencia.

#### 4.6.3.2 Equipamiento de usuario que se deja desatendido

##### **Control**

*“Se recomienda que los usuarios se aseguren que el equipamiento desatendido tenga protección adecuada”<sup>133</sup>*

##### **Relevamiento**

Con el fin de corroborar el cumplimiento de los lineamientos propuestos por el control bajo estudio, se realizaron las siguientes actividades:

- Para verificar el cumplimiento del presente control dentro de la organización se procedió a realizar una entrevista al Jefe del Sector de Sistemas Informáticos, ya que, las estaciones operacionales son responsabilidad de este sector.  
Durante la entrevista se realizaron las siguientes preguntas, en base a lo establecido en el control “*Equipamiento de usuario que se deja desatendido*” de la norma IRAM-ISO/IEC 27002:2008:
  - ¿Se concientiza a los usuarios sobre la importancia de proteger los quipos desatendidos?
  - ¿Qué pautas se dan a los usuarios para proteger los equipos?
- Observación: Se procedió a relevar las instalaciones para determinar cuál es la situación en cuanto al cuidado de los equipos desatendidos.

---

<sup>133</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

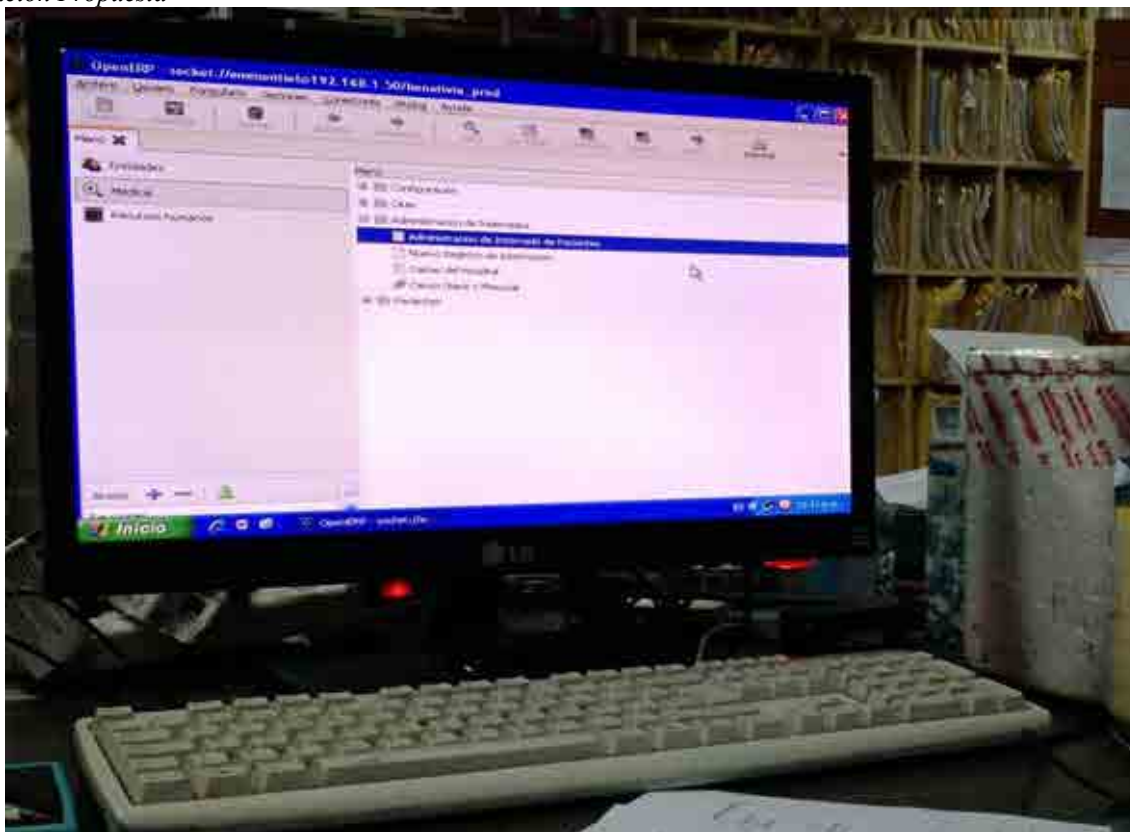


Ilustración 4.6-2

Se puede observar en la imagen un equipo desatendido, el cual tiene una sesión iniciada al sistema ERP de la institución.

En base a la información obtenida durante la entrevista, realizada el día 15/03/2016, y a la observación realizada, se procedió a completar el siguiente checklist

| Equipamiento de usuario que se deja desatendido                                               | Sí | No |
|-----------------------------------------------------------------------------------------------|----|----|
| ¿Se concientiza a los usuarios sobre la protección necesaria a equipos desatendidos?          |    | X  |
| Los usuarios están avisados que deben de:                                                     |    |    |
| Finalizar sesiones activas cuando hayan terminado.                                            |    | X  |
| Utilizar un adecuado método de cierre de sesión (pantalla protegida por contraseña)           |    | X  |
| Se apaguen las computadoras una vez terminada la tarea diaria                                 |    | X  |
| Asegurar las computadoras del uso no autorizado mediante contraseña o un control equivalente. |    | X  |

Tabla 4.6-7

Puede apreciarse en el checklist que en la institución no se concientiza a los usuarios sobre la importancia de proteger los equipos desatendidos, razón por la cual no se cumplimenta con el primer punto del presente control.

Yustman, Mauricio Ezequiel

Pérez Osán, Fernando Javier

Por otro lado, cuando el sector de sistemas informáticos realiza el acondicionamiento de las instalaciones de procesamiento de la información, configura los equipos para que estos se bloqueen mediante contraseña. Esta contraseña es otorgada al usuario y, en caso de ser necesario, se configura una contraseña seleccionada por este. A pesar de esto, los equipos no se bloquean automáticamente cuando estos se dejan desatendidos.

#### 4.6.3.2.1 Cambios recomendados

Para cumplir adecuadamente con las pautas propuestas por el presente control, consideramos que, en primer lugar, debe tenerse en cuenta la solución propuesta en **4.6.5.5.1**(Expiración de la sesión). Tal como se detalla, el “Controlador de Dominio” configurado adecuadamente, ayudará al cierre de sesión y al bloqueo de pantalla, mejorando así la protección de los equipos que se dejan desatendidos. Por otro lado, a pesar de lo antes detallado, consideramos que es necesario concientizar a los usuarios sobre la importancia del cierre de las sesiones activas cuando no se hace uso de los equipos. Para esto recomendamos incluir en la declaración de los derechos de acceso mencionada en **4.6.2.1.1**(Registro de usuarios), un ítem que concientice a los usuarios sobre la importancia de la finalización de la sesión del sistema ERP y recomiende a los usuarios realizar esto una vez terminadas sus tareas en el sistema. Es necesario también incluir en la “*Normativa de uso de los recursos informáticos*” (ver **7.1**) ítems para hacer de público conocimiento la importancia de cerrar las sesiones activas de los sistemas operativos de las estaciones de trabajo una vez finalizada la tarea o bien bloquear el equipo cuando este se deja desatendido (es recomendable que se incluyan guías para realizar esto). Además, es recomendable que se informe la importancia de apagar los equipos cuando se finalizan las tareas diarias.

#### 4.6.3.3 Política de pantalla y escritorio limpio

##### **Control**

*“Se recomienda que se adopte una política de escritorio limpio para los papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de la información”<sup>134</sup>*

##### **Relevamiento**

Con el propósito de examinar el cumplimiento del presente control, se realizó una entrevista a cada uno de los jefes de sector/programa del hospital, dado que, estos son responsable de la información manejada en su sector/programa.

De acuerdo a lo establecido en el control “*Política de pantalla y escritorio limpio*” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante las entrevistas:

- ¿La información sensible o crítica en papel o medios removibles es almacenada bajo llave?
- ¿Las estaciones de trabajo están protegidas mediante contraseña? ¿Las oficinas/instalaciones son protegidas por llave?
- ¿Se protegen los puntos de correo entrante y saliente y los equipos fax?
- ¿Se protege del uso no autorizado a los equipos con tecnología de reproducción (fotocopiadoras, escáneres, etc.)?

---

<sup>134</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

- ¿Cuál es el cuidado que se toma al realizar impresiones con información sensible?

Conforme a los datos obtenidos durante la entrevista realizada el día 15/03/2016, se completó el siguiente Checklist

| Política de pantalla y escritorio limpio                                                               | Sí | No |
|--------------------------------------------------------------------------------------------------------|----|----|
| ¿Existe una política de pantalla y escritorio limpio?                                                  |    | X  |
| Se tienen en cuenta las siguientes directrices (formalmente o informalmente):                          |    |    |
| La información sensible/crítica se debe almacenar en lugares seguros (bajo llave)                      | X  |    |
| Proteger las computadoras con un mecanismo de bloqueo de pantalla y teclado controlado por contraseña. | X  |    |
| Proteger los equipos fax desatendidos                                                                  |    | X  |
| Prevenir el uso no autorizado de tecnologías de reproducción (fotocopiadoras, escáner)                 | X  |    |
| Los documentos con información sensible se deben retirar inmediatamente de impresoras.                 |    | X  |

Tabla 4.6-8

Como puede observarse en el checklist, no existe una política documentada de escritorio y pantalla limpia en la institución, razón por la cual no se cumple con el primer punto del anterior checklist.

Sin embargo, en la institución se aplican de manera informal ciertos controles que se detallan a continuación:

- La información sensible/crítica (en especial la información de historias clínicas e información financiera) se resguarda en armarios bajo llave o es almacenada en sectores a donde esta pertenece.
- Los equipos están protegidos por contraseña (tal cual se detalla en 4.6.5.2 (Identificación y Autenticación de usuarios)).
- Las fotocopiadoras/escáneres que posee la institución solo pueden ser utilizadas por el personal perteneciente al sector donde estas se encuentran. Si una persona ajena al sector requiere utilizarla, debe solicitar autorización al responsable del sector en donde se encuentra el equipo de reproducción.

Por lo detallado previamente consideramos que ciertos puntos del checklist se cumplen dentro de la institución. A pesar de esto, no se aplican controles para proteger los equipos de fax ni se establecen reglas de uso para las impresoras, por lo que concluimos que el presente control se cumple parcialmente dentro de la organización.

#### 4.6.3.3.1 Cambios recomendados

Debido a la inexistencia de una política de pantalla y escritorio limpio y con el objetivo de cumplir con lo propuesto por el presente control, recomendamos que se consideren las siguientes directrices para la elaboración de dicha política:

*Yustman, Mauricio Ezequiel*

- A. Basándose en el Inventario de activos (4.3.1.1.1) y en la clasificación de los mismos (4.3.2.1.1), la información considerada de mayor valor institucional (toda información crítica o sensible) debe ser resguardada en lugares seguros y de acceso restringido.
- B. Protección de los equipos de procesamiento de la información contra accesos no autorizados (Utilizar procedimientos de bloqueo adecuados, como el propuesto en 4.6.5.5.1(Expiración de la Sesión))
- C. Protección de las oficinas de trabajo. Es adecuado que las oficinas de trabajo estén aseguradas bajo llave y el acceso a las mismas sea solo para el personal perteneciente a la institución.
- D. Protección de los equipos de reproducción de documentos (fotocopiadora, escáner). Su uso debe ser restringido y supervisado.
- E. Protección de las Impresoras. Toda información sensible o crítica enviada a estos equipos debe ser retirada de manera rápida por la persona correspondiente.

La política de escritorio y pantalla limpia deber ser elaborada por el comité de seguridad y aprobada por la gerencia del hospital. Es importante que para su elaboración se consideren todos aquellos aspectos de la naturaleza de la institución (hospital público) y la cultura de la misma. Por ejemplo, debe tenerse en cuenta la gran cantidad de gente que accede al hospital y prestar especial atención a la protección de aquellos lugares en donde están a la vista de todos los equipos de trabajo (especialmente en lugares en donde se atiende al público como estadística o arancelamiento)

#### 4.6.4 Control de acceso a la red

*“Objetivo: Prevenir el acceso no autorizado a los servicios de red.*

*Se recomienda que se controle el acceso a los servicios de red, tanto internos como externos.*

*Se recomienda que los accesos de usuarios a la red y servicios de red no comprometan la seguridad de los servicios de red, asegurando que:*

- a) *Existen interfaces apropiadas entre la red de la organización, las redes que son propiedad de otras organizaciones, y las redes públicas.*
- b) *Se aplican mecanismos de autenticación adecuados, para los usuarios y el equipamiento.*
- c) *Se cumple con los controles de acceso de los usuarios a los servicios de información.”<sup>135</sup>*

##### 4.6.4.1 Política de utilización de los servicios de red

#### **Control**

*“Se recomienda que se prevea a los usuarios solo el acceso a los servicios para los cuales han sido específicamente autorizados”<sup>136</sup>*

#### **Relevamiento**

---

<sup>135</sup> IRAM-ISO/IEC 27002:2008

<sup>136</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

Con el fin de corroborar el cumplimiento del presente control en el hospital se realizó una entrevista con el jefe del sector de sistemas informáticos, ya que, es responsabilidad del sector la administración y el mantenimiento de los servicios de red.

Durante la entrevista se realizaron las siguientes preguntas, en base a lo establecido en el control “*Política de utilización de los servicios de red*” de la norma IRAM-ISO/IEC 27002:2008:

- ¿Existe una política referente al uso de los servicios de red?
- ¿Qué aspectos se consideran en la política?

Conforme a los datos obtenidos durante la entrevista realizada al jefe del sector de sistemas informáticos, realizada el día 15/03/2016, se completó el siguiente Checklist:

| Política de utilización de los servicios de red                                                                 | Sí | No |
|-----------------------------------------------------------------------------------------------------------------|----|----|
| ¿Existe una política concerniente al uso de la red y los servicios de red?                                      |    | X  |
| Para la gestión de la redes se tiene en cuenta:                                                                 |    |    |
| Redes y servicios a los cuales se permite el acceso                                                             | X  |    |
| Procedimiento de autorización para determinar que personas tienen permisos de acceso a qué red y a qué servicio | X  |    |
| Controles y procedimientos de gestión para proteger el acceso a las conexiones y servicio de red                | X  |    |
| Los medios utilizados para acceder a las redes y servicios de red                                               | X  |    |

Tabla 4.6-9

Puede apreciarse en el checklist que la institución no posee una política para la utilización de los servicios de red. A pesar de esto, es necesario aclarar que existen dos servicios de red claramente definidos en la institución, un servicio de red inalámbrica y un servicio de red alámbrico, el primero está destinado para el uso de dispositivos móviles (celular, Tablets, notebooks) mientras que el segundo es exclusivo para el uso de las estaciones de trabajo (PCs de escritorio de la institución). El uso de ambas redes está correctamente reglamentada y controlada. Las redes son gestionadas de la siguiente forma:

- La red alámbrica está destinada para el uso laboral y se encuentra reglamentada por la Normativa de uso de los recursos informáticos (ver 7.1). Las reglas de uso de esta red están definidas en dicha normativa. Todos los equipos conectados a esta red están identificados por una dirección IP y un nombre de red propio (esta IP y Nombre son configurados por el sector de sistemas informáticos al momento de introducir el equipo en la red laboral de la institución). Todas las IPs de los equipos se encuentran registrados en el firewall destinado a esta red, ayudando así, a que solo los equipos autorizados hagan uso de la misma, y además se configuran los permisos de acceso para cada una de las direcciones IP. A sí mismo, se administran permisos especiales (de acceso a sitios determinados) otorgados según la necesidad del usuario y previa autorización del sector del sistema informáticos.
- La red inalámbrica está destinada para el uso de dispositivos móviles (celulares, Tablets, notebooks) personales y se encuentra reglamentada por las condiciones de uso de la

misma. Estas condiciones de uso (ver 7.4) son entregadas al usuario. El acceso a esta red es otorgado según el procedimiento detallado en 4.2.1.4 (Proceso para la autorización de equipos personales). Esta red también posee un firewall propio, lo que ayuda a identificar a cada uno de los usuarios que hacen uso de esta red (los usuarios están identificados por un nombre propio otorgado cuando se brinda acceso a esta red). Es importante destacar que esta red es independiente de la red laboral (no existe comunicación posible entre ambas redes). Esta red no posee restricciones de acceso, por lo tanto, los usuarios pueden hacer un uso libre de la misma. Por último, es necesario destacar que se aplican controles para gestionar el tráfico de la misma y así ayudar a mejorar el servicio brindado por esta.

Según lo detallado previamente, consideramos que, a pesar de la inexistencia de una política general concerniente al uso de la red y de los servicios de red, el presente control se cumple parcialmente en la institución ya que existen reglas y controles que se aplican a cada una de las redes disponibles.

#### 4.6.4.1.1 Cambios recomendados

A pesar de la existencia de controles y reglas que se aplican a cada una de las redes disponibles en el hospital que ayudan a una gestión más ordenada de las mismas, consideramos que para cumplimentar adecuadamente lo propuesto por el presente control se debe elaborar una política de utilización de los servicios de red en donde se detalle:

- Las redes y servicios disponibles a los cuales el personal de la institución tiene permitido acceder.
- Deben aclararse para cada una de las redes las limitaciones de acceso que posee cada servicio (limitaciones de uso, descargas, páginas restringidas, etc.)
- Aclarar los procedimientos de autorización para poder hacer uso de las redes disponibles.
- Controles a utilizar para gestionar adecuadamente los servicios y poder brindar un servicio de calidad.

Debe incluirse en esta política toda la información que se considere necesaria que detalle la manera en la que actualmente se gestionan las redes.

La política debe ser elaborada por el sector de sistemas informáticos en colaboración con el responsable de seguridad de la información. La misma debe ser aprobada por el comité de seguridad de la información y por la gerencia del hospital.

#### 4.6.4.2 Autenticación de usuarios para conexiones externas

##### **Control**

*“Se recomienda que se utilice métodos de autenticación apropiados para el control de acceso de usuarios remotos”<sup>137</sup>*

##### **Relevamiento**

Para verificar el cumplimiento del presente control dentro de la organización se procedió a realizar una entrevista al Jefe del Sector de Sistemas Informáticos, ya que, es responsabilidad del sector la administración y el mantenimiento de los servicios de red.

---

<sup>137</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

Teniendo en cuenta lo establecido en el control “Autenticación de usuarios para conexiones externas” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:

- ¿Se utilizan conexiones externas? ¿Cómo se realiza la autenticación de usuarios remotos?
- ¿Qué controles se aplican para gestionar las conexiones remotas?

En base a la información obtenida durante la entrevista, se determinó que en el hospital (por política interna del sector de sistemas informáticos y por razones de seguridad) las conexiones de usuarios remotos no están permitidas, por lo tanto, no se realizó el estudio del presente control en la institución.

#### 4.6.4.2.1 Consideraciones de control

Si bien las conexiones de usuarios remotos no están permitidas en la institución, consideramos que este tipo de conexión debe tenerse en cuenta, de manera tal de estar preparado en caso de ser necesaria. Para esto recomendamos la utilización de herramientas que permitan establecer una conexión VPN, esto ayudara a establecer una conexión segura entre dos puntos. Debe evaluarse la necesidad de uso y las características de la conexión para seleccionar la herramienta a utilizar (Actualmente existen una gran cantidad de herramientas para poder establecer una VPN)

#### 4.6.4.3 Identificación del equipamiento en la red

##### **Control**

*“Se recomienda que se considere la identificación automática de equipamiento como un medio para autenticar conexiones de ubicaciones y equipamiento específicos”<sup>138</sup>*

##### **Relevamiento**

Con el propósito de examinar el cumplimiento del presente control, se realizó una entrevista al Jefe del Sector de Sistemas Informáticos, dado que, es este sector el encargado de gestionar las redes de la institución.

Durante la entrevista se consultó al jefe del sector sobre la forma mediante la cual son identificados los equipos de la red. En base a la información obtenida, se determinó que en la institución se identifican a todos los equipos conectados a los servicios de red disponible de la siguiente manera:

- A. Red alámbrica (red laboral): todos los equipos conectados a esta red están identificados por un número de dirección IP único y un nombre de red único. Estas direcciones IP son ingresadas en el firewall destinado para esta red.  
A continuación, se muestra una imagen en la cual podemos observar grupos de usuario (divididos por sector)

---

<sup>138</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

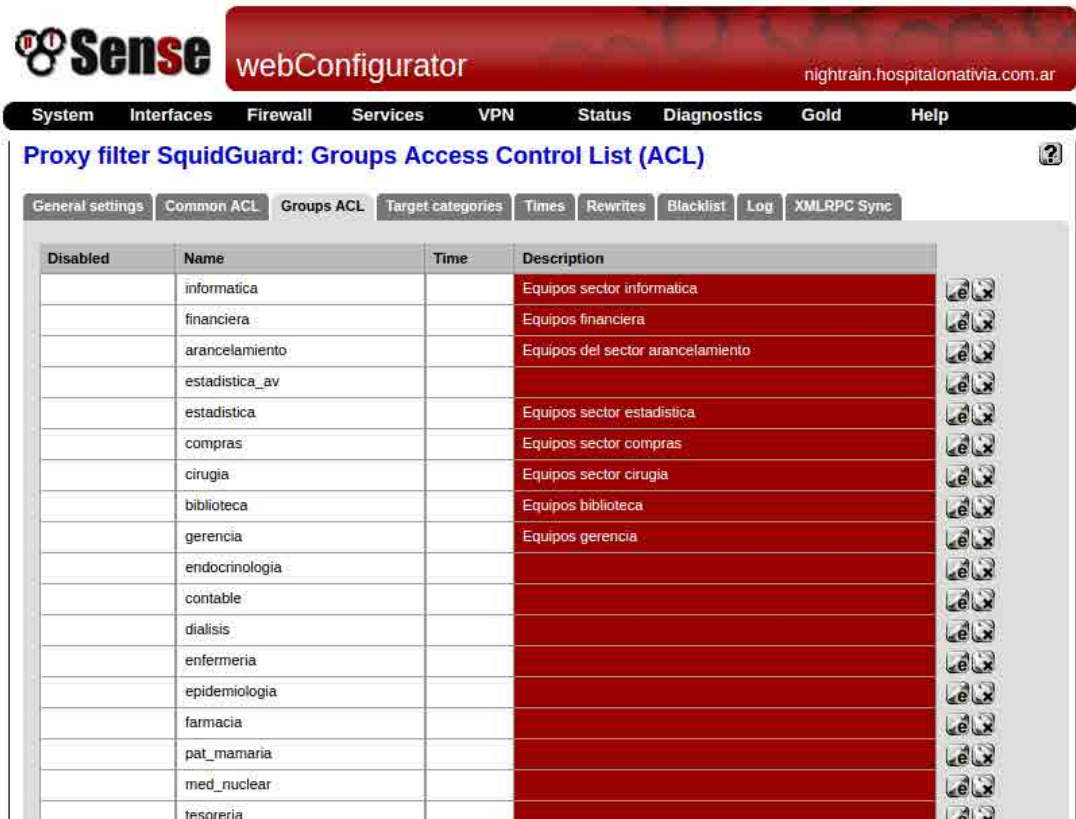


Ilustración 4.6-3

Dentro de cada grupo están las direcciones IP de las máquinas que conforman ese grupo (la imagen de las maquinas que conforman cada grupo no fue incluida debido al carácter confidencial de esta información).

- B. Red inalámbrica (dispositivos móviles): En el caso de la red inalámbrica no se identifican los dispositivos conectados, sino que se identifican a los usuarios que están haciendo uso de este servicio (nombre de usuario único otorgado). Estos usuarios conectados están asociados a una dirección IP que permite controlar la actividad de la misma.

A continuación, se muestra una imagen en la cual podemos observar como son identificados todos los usuarios que están haciendo uso de esta red.

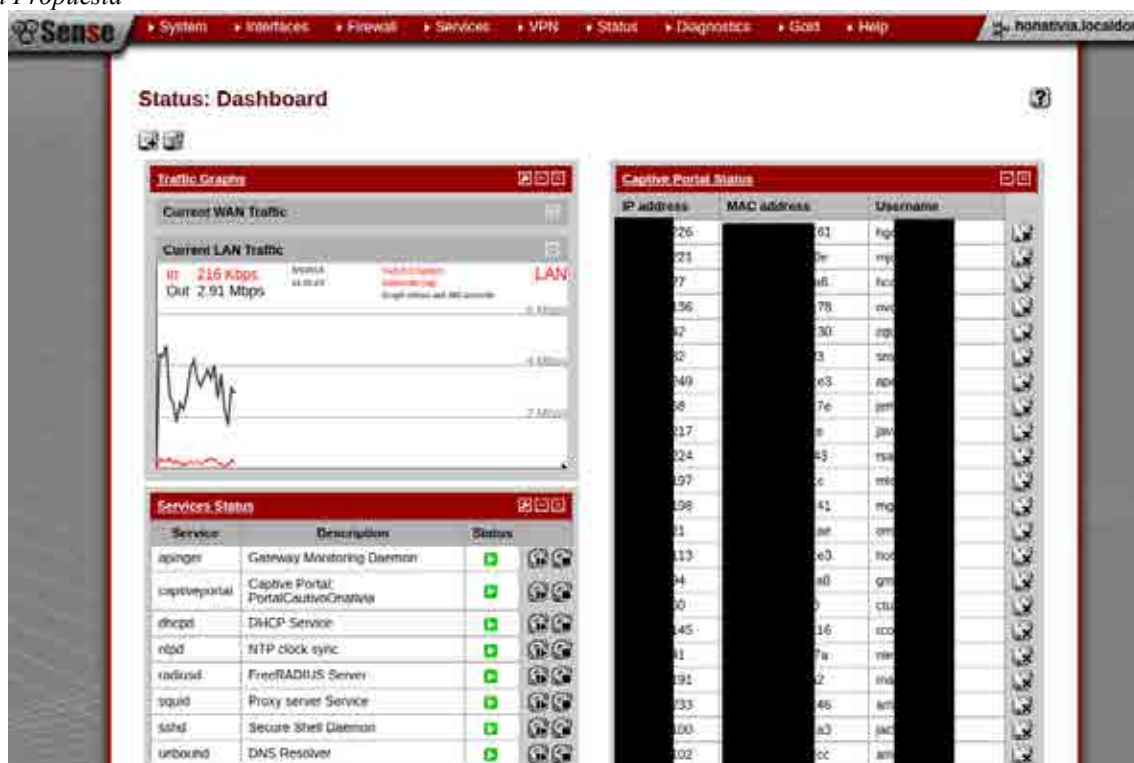


Ilustración 4.6-4

Es necesario destacar que ambos servicios poseen un rango de direcciones IP y una máscara de subred diferentes, lo que ayuda a identificar a que red está conectada el equipo.

En cuanto a los equipos de red (routers/switches), estos son adecuadamente identificamos, ya que, al momento de realizar la configuración, se registra la dirección IPs y MAC del mismo en un documento digital.

Debido a lo detallado previamente consideramos que le presente control se cumple adecuadamente en la institución.

#### 4.6.4.4 Protección de los puertos de diagnóstico y configuración remotos

##### **Control**

*“Se recomienda que se controles el acceso físico y lógico a los puertos de diagnóstico y de configuración”<sup>139</sup>*

##### **Relevamiento**

Con el fin de corroborar el cumplimiento del presente control en el hospital se realizó una entrevista con el jefe del sector de sistemas informáticos, ya que, es responsabilidad del sector el mantenimiento de las redes.

Durante la entrevista se consultó al jefe del sector sobre las medidas que se tienen en cuenta para la protección de los puertos de diagnóstico y configuración remotos. Se determinó que, no se aplican controles especiales para proteger estos puertos; solamente se protegen los equipos de la red lógicamente (mediante contraseña). Esto se debe principalmente a que, en muchos de los casos, el equipamiento utilizado no posee estos puertos (ya que en su mayoría

<sup>139</sup> IRAM-ISO/IEC 27002:2008  
 Yustman, Mauricio Ezequiel

son equipos que no tienen características empresariales) y, por otro lado, el equipamiento de mayor importancia (routers y switches de mayor capacidad e importancia) se encuentra físicamente en el sector.

Por otro lado, se pudo observar en las instalaciones de la institución que existen diferentes equipos de red (Routers, Switches) visibles en las diferentes áreas del hospital, lo que puede generar problemas ya que se encuentran al alcance de cualquier persona.



Ilustración 4.6-5

Se pudo observar también que los racks de redes existentes en la organización no están asegurados por llave. Es importante aclarar que el rack de mayor importancia se encuentra dentro de las oficinas del sector de sistemas informáticos (la oficina está asegurada con llave)

#### 4.6.4.4.1 Cambios recomendados

Considerando que el equipamiento existente en la organización no posee puertos de diagnóstico y configuración, con el objetivo de cumplimentar con lo propuesto por el presente control, recomendamos que:

- Para la protección lógica de los equipos de Red, se utilicen contraseñas seguras y para la selección y uso de las mismas se consideren las recomendaciones mencionadas en 7.5 (Guía de buenas prácticas para el uso de contraseñas). Estas contraseñas deben ser manejadas únicamente por el correspondiente administrador de Redes. Es importante considerar además que, algunos equipos de red, permiten acceder a la configuración de estos de manera remota, es por esto que los equipos deben configurarse de manera tal que solo un equipo conectado a la red a la cual pertenece el equipo de red pueda acceder a su configuración. En la mayoría de los equipos de red esta configuración viene por defecto, aun así, recomendamos garantizar que la configuración sea la apropiada.
- Para la protección física de los equipos, recomendamos por un lado que, aquellos racks de la institución que poseen equipos de red, sean asegurados debidamente bajo llave. Por otro lado, es importante bloquear (en caso de ser posible realizarlo a través del menú de configuración del equipo de red) los puertos LAN que no estén siendo utilizados de los Routers/Switches que están al alcance de cualquier persona. En caso de que no sea posible realizar el bloqueo mediante un cambio de configuración, recomendamos realizar el bloqueo de estos físicamente. Recomendamos utilizar la herramienta LockIT de Siemon (más información [http://www.siemon.com/es/company/press\\_releases/09-01-05-lockit.asp](http://www.siemon.com/es/company/press_releases/09-01-05-lockit.asp)) o similares para bloquear físicamente los puertos LAN en desuso.

### **Control**

*“Se recomienda que los grupos de servicios de la información, usuarios y sistemas de información se subdividan en redes”<sup>140</sup>*

### **Relevamiento**

Con el objeto de examinar el cumplimiento del presente control en la organización, se realizó una entrevista al Jefe del Sector de Sistemas Informáticos, debido a que el diseño, implementación, mantenimiento y control de las redes de datos del Hospital son responsabilidad de dicho sector.

En base a lo establecido en el control “*Separación en Redes*” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:

- ¿La red del Hospital se encuentra separada de la red Pública? ¿De qué manera se encuentra separada?
- ¿La red del Hospital se encuentra separada o subdividida? ¿De qué manera?
- ¿Cada uno de los dominios de red se define en base a una evaluación de riesgos?
- ¿Se establecen controles para cada dominio de red?
- ¿Qué criterios se tienen en cuenta para subdividir la red? ¿Qué métodos/funcionalidades se emplean para subdividir la red?

Conforme a los datos obtenidos durante la entrevista realizada al Jefe del Sector de Sistemas Informáticos, realizada el día 15/03/2016, se completó el siguiente Checklist:

| Separación de Redes                                                                                                            | Si | No |
|--------------------------------------------------------------------------------------------------------------------------------|----|----|
| La red LAN de la organización se encuentra separada de la red externa mediante un “Firewall” o a través de un “Gateway”        | X  |    |
| La red interna del Hospital se encuentra subdividida en subredes o bien existen redes virtuales para cada grupo de usuarios    |    | X  |
| Se define un perímetro de seguridad para cada dominio de red interno                                                           |    | X  |
| Se define un conjunto de controles a aplicar para cada dominio de red existente                                                | X  |    |
| Los dominios de red se definen en base a una evaluación de riesgos y en base a los requerimientos de seguridad de cada dominio |    | X  |
| Al momento de subdividir la red, se tienen en cuenta los siguientes criterios:                                                 |    |    |
| Políticas de control de acceso                                                                                                 |    | X  |
| Requerimientos de acceso                                                                                                       |    | X  |
| Impacto sobre el desempeño de la red                                                                                           |    | X  |
| Clasificación de la información que trafica en la misma                                                                        |    | X  |

<sup>140</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

|                                                                                                                                                     |   |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|---|---|
| Las redes se dividen a través de funcionalidades de los dispositivos de red                                                                         |   | X |
| La red inalámbrica del hospital se encuentra separada de la red alámbrica                                                                           | X |   |
| En el caso de las redes inalámbricas se realiza una evaluación de riesgos con el propósito de determinar los controles a implementar sobre la misma |   | X |

Tabla 4.6-10

Podemos ver en el Checklist anterior que la red del Hospital se encuentra separada de la red Pública mediante un Firewall, sin embargo, no se subdivide en dominios o subredes diferentes. Cabe destacar que, la red alámbrica del Hospital se encuentra separada de la red inalámbrica (ver 4.6.4.1(Política de utilización de los servicios de red)), y el jefe de cada una de las áreas de la Organización establecen cuales empleados tienen acceso a la red, por lo que consideramos que, si se establecen controles, si bien no para cada dominio de red, para cada sector de la Institución.

#### 4.6.4.5.1 Cambios Recomendados

Recomendamos, para lograr un adecuado cumplimiento de lo establecido por el presente control, la implementación de Redes de Área Local Virtuales (VLAN), lo cual permite subdividir la red en redes virtuales separadas, logrando de esta manera mejorar la gestión de la red de la organización y limitar el dominio de difusión, sin la necesidad de adquirir nuevos equipos de red. Cabe destacar que el firewall actualmente disponible en el Hospital es compatible con esta tecnología. Es recomendable que la red se subdivida teniendo en cuenta los siguientes criterios:

- Los programas/sectores del Hospital
- Políticas de control de accesos.
- Requerimientos de acceso a la red
- Desempeño de la red
- Información transmitida

Recomendamos que, antes de realizar la subdivisión, se realice una evaluación de los riesgos implicados en dicha subdivisión. La misma debe ser realizada por el responsable de la seguridad de la Información.

Consideramos que la subdivisión debe ser realizada únicamente para la red alámbrica del Hospital, debido a que la red inalámbrica no es empleada para propósitos estrictamente laborales (tal como se establece en 7.4(condiciones de uso del servicio wifi)), y por ello, no es necesario aplicar controles tan estrictos sobre la misma.

#### 4.6.4.6 Control de Conexión a la Red

##### **Control**

*“Para redes compartidas, especialmente aquellas que se extienden a través de los límites de la organización, se recomienda que se restrinja la capacidad de los usuarios para conectarse a la red, en línea con la política de control de acceso y con los requerimientos de las aplicaciones de la actividad”<sup>141</sup>*

<sup>141</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

### **Relevamiento**

Con el fin de corroborar el cumplimiento de los lineamientos propuestos por el control bajo estudio, se realizaron las siguientes actividades:

- Entrevista al Jefe del Sector de Sistemas Informáticos, ya que las restricciones de acceso a la red son establecidas por dicho sector.  
 Teniendo en cuenta lo establecido en el control “Control de conexión a la red” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:
  - ¿Se otorga acceso a la red mediante un usuario y contraseña?
  - ¿Los privilegios de acceso son revisados y actualizados cada intervalo regular de tiempo? ¿Este tiempo se encuentra definido en la política de control de accesos?
  - ¿Se filtra el tráfico de red? ¿Cuál es el contenido filtrado?
- Observación: se solicitó al jefe del sector de sistemas informáticos poder visualizar las diferentes herramientas utilizadas para el control de la red (firewall) y sus respectivas configuraciones.

Tal como se establece en 4.6.4.1 (Política de utilización de los servicios de red), coexisten 2 redes diferentes dentro del Hospital, una alámbrica, utilizada por las estaciones de trabajo, y otra inalámbrica, destinada a los dispositivos móviles de los empleados. Cada una de las mismas posee su propio Firewall e ISP, por lo que se procedió a evaluar los puntos de la norma para cada una por separado.

### **Red Alámbrica**

Conforme a los datos obtenidos durante la entrevista realizada al jefe del sector de sistemas informáticos, realizada el día 15/03/2016, se completó el siguiente Checklist:

| Control de conexión a la red                                                                                                                                                          | Si | No |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|
| Se otorga acceso a la red de la organización mediante un usuario y una contraseña                                                                                                     |    | X  |
| Los derechos de acceso de los usuarios se actualizan cada intervalos regulares de tiempo, o bien cuando ocurren cambios significativos (Por ej.: un empleado abandona la institución) |    | X  |
| Las políticas de control de acceso establecen el intervalo de tiempo tras el cual se deben actualizar los derechos de acceso de los usuarios                                          |    | X  |
| Se filtra o restringe el tráfico de:                                                                                                                                                  |    |    |
| Mensajería (Por ej.: El correo electrónico o las redes sociales)                                                                                                                      |    | X  |
| Transferencia de Archivos (Por ej.: descarga de archivos)                                                                                                                             | X  |    |
| Acceso interactivo (Por ej.: YouTube y redes sociales)                                                                                                                                | X  |    |
| Acceso a aplicaciones (Por ej.: Spotify o juegos en línea)                                                                                                                            | X  |    |

Tabla 4.6-11

Como podemos apreciar en el Checklist anterior no es necesario un usuario y contraseña para el acceso a la red alámbrica del Hospital y, tal como se indica en **4.6.4.1**(Política de utilización de los servicios de red), las direcciones de red de las estaciones de trabajo se encuentran registradas en el firewall, de manera tal que únicamente las estaciones registradas puedan hacer uso de la red alámbrica del Hospital. Por otro lado, el firewall de la organización establece una serie de filtros para la transferencia de archivos, el acceso interactivo (Por ejemplo, Facebook o YouTube), y otras aplicaciones que consumen ancho de banda (Por ejemplo, Ares o BitTorrent). Finalmente, los derechos de acceso a la red no son actualizados cada intervalo regular de tiempo o bien cuando un empleado abandona la organización, ya que, tal como se indica en **4.4.3.3**(Remoción de Derechos de Acceso), no se notifica al sector de informática cuando una persona abandona el Hospital.

A continuación, se muestra una imagen en donde podemos observar las diferentes restricciones que pueden ser configuradas a través del firewall.

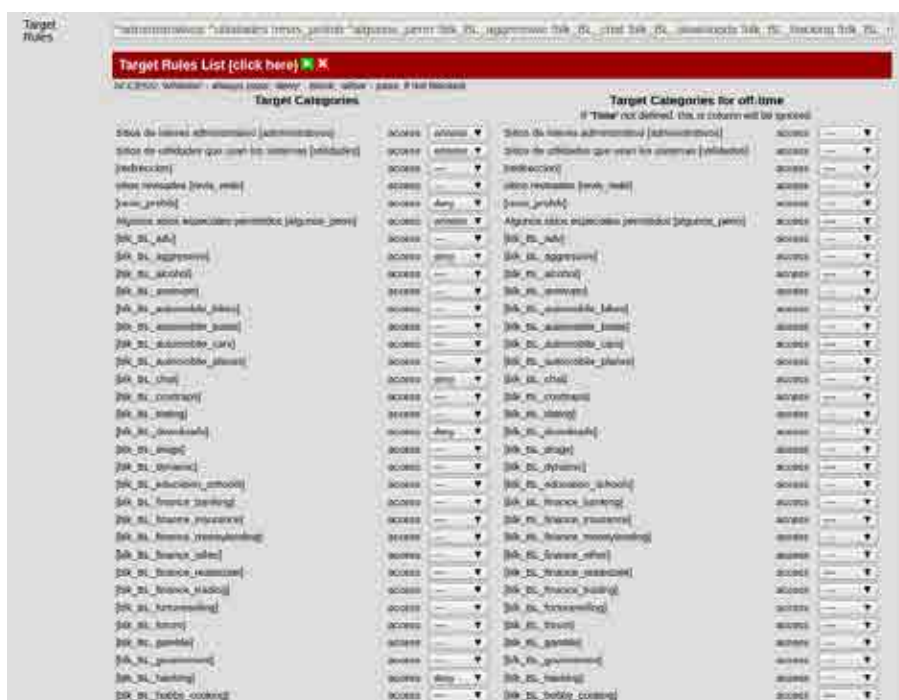


Ilustración 4.6-6

### **Red Inalámbrica**

Conforme a los datos obtenidos durante la entrevista realizada al jefe del sector de sistemas informáticos, realizada el día 15/03/2016, se completó el siguiente Checklist:

|                                                                                                                                                                                       |    |    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|
| Control de conexión a la red                                                                                                                                                          | Si | No |
| Se otorga acceso a la red de la organización mediante un usuario y una contraseña                                                                                                     | X  |    |
| Los derechos de acceso de los usuarios se actualizan cada intervalos regulares de tiempo, o bien cuando ocurren cambios significativos (Por ej.: un empleado abandona la institución) |    | X  |

|                                                                                                                                              |  |   |
|----------------------------------------------------------------------------------------------------------------------------------------------|--|---|
| Las políticas de control de acceso establecen el intervalo de tiempo tras el cual se deben actualizar los derechos de acceso de los usuarios |  | X |
| Se filtra o restringe el tráfico de:                                                                                                         |  |   |
| Mensajería (Por ej.: El correo electrónico o las redes sociales)                                                                             |  | X |
| Transferencia de Archivos (Por ej.: descarga de archivos)                                                                                    |  | X |
| Acceso interactivo (Por ej.: YouTube y redes sociales)                                                                                       |  | X |
| Acceso a aplicaciones (Por ej.: Spotify o juegos en línea)                                                                                   |  | X |

Tabla 4.6-12

Puede observarse en el Checklist anterior que se otorga a cada empleado de la organización un usuario y una contraseña para acceder a la red inalámbrica del Hospital. Sin embargo, no se revisan los derechos de acceso ni se dispone de una política de control de accesos que establezca los intervalos cada los que deben realizarse los mismos. Por otra parte, no se establece ningún tipo de filtro en el tráfico; esto se debe a que, la misma se encuentra destinada a los dispositivos móviles que son propiedad de los empleados del Hospital, y es de uso personal. Es necesario destacar que existen limitaciones al consumo del ancho de banda de la red, de manera que la misma no se congestione por el elevado consumo de pocos dispositivos.

A continuación, se muestran imágenes capturadas con un dispositivo móvil en la cual se visualiza el control existente (portal cautivo) para acceder a esta red:



Ilustración 4.6-7

#### 4.6.4.6.1 Cambios Recomendados

En primer lugar, para cumplir con lo establecido por la norma, sugerimos que, en la política de control de accesos, mencionada en 4.6.1.1.1 (Política de control de accesos), se establezcan los intervalos cada los que deben revisarse los derechos de acceso a la red del Hospital. Recomendamos que se asigne la responsabilidad de dichas revisiones al responsable de Seguridad de la Información.

En el caso específico de la red alámbrica, consideramos que no es necesario brindar un usuario y contraseña para acceder a la red, ya que este tipo de solución podría ser incompatible con otras soluciones propuestas, como por ejemplo la mencionada en 4.6.5.1.1 (Procedimientos seguros de inicio de sesión). Sin embargo, si consideramos que el tráfico de mensajería debe filtrarse, por lo que es necesario configurar adecuadamente el firewall de la organización para filtrar los correos electrónicos y las redes sociales.

Finalmente, consideramos que, en el caso de la red inalámbrica, al encontrarse destinada al uso personal de los empleados del hospital, no es necesario implementar filtros de contenido. (Consideramos que la medida actual de controlar el tráfico de la misma para brindar un servicio aceptable es suficiente para el caso)

#### 4.6.4.7 Control de enrutamiento de red

##### **Control**

*“Se recomienda que se implementen en las redes controles de enrutamiento para garantizar que las conexiones informáticas y los flujos de información no violen la política de control de acceso de las aplicaciones del negocio.”<sup>142</sup>*

##### **Relevamiento**

Con el fin de corroborar el cumplimiento del presente control en el hospital se mantuvo una entrevista con el jefe del sector de sistemas informáticos, ya que consideramos que los controles de enrutamiento en las redes son responsabilidad el sector anteriormente mencionado.

Durante la entrevista se realizaron las siguientes preguntas, en base a lo establecido en el control “Control de enrutamiento de red” de la norma IRAM-ISO/IEC 27002:2008:

- ¿Existen controles que permiten validar las direcciones de origen y destino de los paquetes que circulan en la red? ¿Cuáles son estos controles?
- ¿Se emplean tecnologías de traducción de direcciones de red o “proxys”? ¿Se tienen conocimientos acerca de las fortalezas y debilidades de estas tecnologías?
- ¿El control de enrutamiento se basa en la política de control de accesos?

En base a la información obtenida durante la entrevista, realizada el día 15/03/2016, se procedió a completar el siguiente Checklist

| Control de enrutamiento de red                                                                         | Si | No |
|--------------------------------------------------------------------------------------------------------|----|----|
| Las puertas de enlace o los “Firewalls” validan las direcciones de origen y de destino de los paquetes | X  |    |

<sup>142</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

|                                                                         |   |   |
|-------------------------------------------------------------------------|---|---|
| Se emplean tecnologías de traducción de direcciones y/o “proxys”        | X |   |
| El control de enrutamiento se basa en la política de control de accesos |   | X |

Tabla 4.6-13

Podemos contemplar en el Checklist anterior que existen tecnologías que validan las direcciones de origen y destino de los paquetes de red. Específicamente, el Hospital dispone de dos Firewalls (uno de ellos para la red alámbrica y otro para la inalámbrica) que verifican las direcciones de origen y destino de los paquetes que ingresan de la red pública a la red de área local y viceversa. Por otro lado, los mismos también controlan la dirección de origen y destino de los paquetes de la red LAN, con el objetivo de descartar todos los paquetes que tengan su origen en la red inalámbrica y su destino en la alámbrica, o viceversa.

Por otro lado, se utilizan “proxys” tanto en la red inalámbrica como alámbrica. En la primera, se emplea un “proxy transparente”, por lo que no es necesario configurar por separado cada uno de los dispositivos móviles conectados, para controlar el tráfico, mientras que en la segunda se emplea un “proxy explícito”, por lo que los hosts conectados a la red alámbrica deben conocer cuál es el puerto habilitado para navegar a través de internet.

Finalmente, como se explica en 4.6.1.1(Política de control de accesos), no existe una política de control de accesos en el Hospital. Por estas razones, consideramos que no se cumple con el último punto del Checklist presentado anteriormente.

#### 4.6.4.7.1 Cambios Recomendados

Es recomendable que, una vez desarrollada la política de Control de Accesos, elaborada en 4.6.1.1(Política de control de accesos), en caso de ser necesario, se adecue el control de enrutamiento actualmente existente en la organización. Sin embargo, consideramos que el control actualmente implementado es suficiente para la organización.

#### 4.6.5 Control de acceso al sistema operativo

*“Objetivo: Prevenir el acceso no autorizado a los sistemas operativos.*

*Se recomienda que se utilicen las instalaciones de seguridad para restringir el acceso a los sistemas operativos solo a los usuarios autorizados. Se recomienda que los recursos sean capaces de lo siguiente:*

- Autenticar a los usuarios autorizados, en relación con la política de control de acceso definida.*
- Registrar los intentos de autenticaciones del sistema, exitosas y fallidas.*
- Registrar el uso de privilegios especiales del sistema.*
- Emitir alarmas cuando se violen las políticas de seguridad del sistema.*
- Prever medios apropiados para la autenticación.*
- Cuando sea apropiado, restringir el tiempo de conexión de los usuarios”<sup>143</sup>*

<sup>143</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

### **Control**

*"Se recomienda que el acceso a los sistemas operativos se controle por un procedimiento seguro de inicio de sesión."*<sup>144</sup>

### **Relevamiento**

Con el fin de corroborar el cumplimiento de los lineamientos propuestos por el control bajo estudio, se realizaron las siguientes actividades:

- Entrevista al Jefe del Sector de Sistemas Informáticos, dado que, es este sector el encargado de configurar los sistemas operativos de los dispositivos que son propiedad del Hospital  
 De acuerdo a lo establecido en el control "*Procedimientos seguros de inicio de sesión*" de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:
  - ¿Los sistemas operativos de los servidores/clientes cuentan con procedimientos para el inicio de sesión?
  - ¿Qué información muestra la pantalla de inicio de sesión? ¿Qué información se muestra en caso que el ingreso sea fallido?
  - ¿Se limitan la cantidad de intentos fallidos? ¿Se lleva registro de los mismos? ¿Se establece un tiempo de retraso antes de permitir nuevos intentos de inicio de sesión?
  - ¿Se toma algún tipo de medida especial al alcanzar el número máximo de intentos fallidos (Por ejemplo, bloquear la conexión o el envío de alertas al administrador del sistema)?
  - ¿La contraseña se encuentra oculta? ¿Se transmite como texto limpio?
  - ¿Qué información se muestra cuando se completa el ingreso al sistema?
- Observación: se precedió a visualizar el método de inicio de sesión en las máquinas de usuario (10 PCs, en las cuales el inicio de sesión era el mismo, ya que se solicitaba contraseña y usuario para acceder) y en los servidores disponibles en la institución.

Es necesario destacar en este punto que, se evaluaron por separado el cumplimiento de los controles para los sistemas Operativos de los clientes y de los servidores, por lo que a continuación, se exponen los resultados obtenidos para cada uno:

### **Sistemas Operativos de las Terminales de tipo "Cliente"**

Conforme a los datos obtenidos durante la entrevista realizada el día 15/03/2016, se completó el siguiente Checklist:

| Procedimientos seguros de inicio de sesión (clientes)                                 | Si | No |
|---------------------------------------------------------------------------------------|----|----|
| El sistema operativo cuenta con un procedimiento para el inicio de sesión en el mismo | X  |    |
| El procedimiento no muestra ningún tipo de información relevante                      |    | X  |

<sup>144</sup> IRAM-ISO/IEC 27002:2008  
 Yustman, Mauricio Ezequiel

|                                                                                                                                                                                          |   |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|
| El procedimiento de inicio de sesión:                                                                                                                                                    |   |   |
| No muestra identificadores de sistema o de aplicaciones en pantalla, hasta que se completa el inicio de sesión                                                                           | X |   |
| Muestra una nota indicando que solo pueden ingresar usuario debidamente autorizados                                                                                                      |   | X |
| No provee mensajes de ayuda durante el ingreso al sistema                                                                                                                                |   | X |
| No valida ningún tipo de información de inicio, hasta que se completa el proceso de ingreso                                                                                              | X |   |
| En caso que los datos ingresados sean erróneos, no indica que datos son correctos y cuales incorrectos (Por ejemplo, no indica que el usuario es correcto y la contraseña es incorrecta) | X |   |
| Limita el nº de ingresos fallidos permitidos al sistema                                                                                                                                  |   | X |
| Registra los intentos fallidos y exitosos al sistema                                                                                                                                     |   | X |
| Establece un tiempo de retraso antes de permitir nuevos intentos de inicio de sesión, o bien rechace futuros intentos sin autorización específica                                        |   | X |
| Se desconecte de las conexiones de vínculos de datos, en caso que se superen el número de intentos permitidos                                                                            |   | X |
| Envíe un mensaje de alerta en el caso que se alcance el máximo número de intentos permitidos                                                                                             |   | X |
| No transmite la contraseña como texto limpio                                                                                                                                             |   | X |
| Oculto la contraseña                                                                                                                                                                     | X |   |
| Establece el número de reintentos de ingreso de contraseñas                                                                                                                              |   | X |
| Limita el tiempo máximo y mínimo para el procedimiento de ingreso al sistema                                                                                                             |   | X |
| Al completarse el ingreso muestra:                                                                                                                                                       |   |   |
| Fecha y hora del ultimo ingreso exitoso                                                                                                                                                  |   | X |
| Detalle de cualquier ingreso fallida desde el último ingreso                                                                                                                             |   | X |

Tabla 4.6-14

Se puede observar en el Checklist anterior que, para los equipos clientes (Computadoras de Escritorio), se dispone de un procedimiento de inicio de sesión para el sistema operativo, el cual, consideramos que muestra información relevante al mostrar los usuarios con los que es posible acceder al sistema. A pesar de esto, no se muestran indicadores o aplicaciones relevantes en pantalla, ni permite realizar ningún tipo de actividad hasta completado el proceso de inicio de sesión. Tampoco indica que datos son correctos e incorrectos, en caso que se ingresen erróneamente los datos de inicio, y oculta la contraseña en pantalla. Cabe destacar, que las computadoras del Hospital no se encuentran correctamente configuradas para registrar eventos

fallidos de inicio de sesión, ni limitan el número de ingresos fallidos al sistema, y, en consecuencia, no se cumplimentan numerosos puntos del presente control.

### **Sistemas Operativos de los Servidores**

| Procedimientos seguros de inicio de sesión (Servidores)                                                                                                                                  | Si | No |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|
| El sistema operativo cuenta con un procedimiento para el inicio de sesión en el mismo                                                                                                    | X  |    |
| El procedimiento no muestra ningún tipo de información relevante                                                                                                                         | X  |    |
| El procedimiento de inicio de sesión:                                                                                                                                                    |    |    |
| No muestra identificadores de sistema o de aplicaciones en pantalla, hasta que se completa el inicio de sesión                                                                           | X  |    |
| Muestra una nota indicando que solo pueden ingresar usuario debidamente autorizados                                                                                                      |    | X  |
| No provee mensajes de ayuda durante el ingreso al sistema                                                                                                                                | X  |    |
| No valida ningún tipo de información de inicio, hasta que se completa el proceso de ingreso                                                                                              | X  |    |
| En caso que los datos ingresados sean erróneos, no indica que datos son correctos y cuales incorrectos (Por ejemplo, no indica que el usuario es correcto y la contraseña es incorrecta) | X  |    |
| Limita el nº de ingresos fallidos permitidos al sistema                                                                                                                                  |    | X  |
| Registra los intentos fallidos y exitosos al sistema                                                                                                                                     | X  |    |
| Establece un tiempo de retraso antes de permitir nuevos intentos de inicio de sesión, o bien rechace futuros intentos sin autorización específica                                        |    | X  |
| Se desconecte de las conexiones de vínculos de datos, en caso que se superen el número de intentos permitidos                                                                            |    | X  |
| Envíe un mensaje de alerta en el caso que se alcance el máximo número de intentos permitidos                                                                                             |    | X  |
| No transmite la contraseña como texto limpio                                                                                                                                             | X  |    |
| Oculto la contraseña                                                                                                                                                                     | X  |    |
| Establece el número de reintentos de ingreso de contraseñas                                                                                                                              |    | X  |
| Limita el tiempo máximo y mínimo para el procedimiento de ingreso al sistema                                                                                                             |    | X  |
| Al completarse el ingreso muestra:                                                                                                                                                       |    |    |
| Fecha y hora del ultimo ingreso exitoso                                                                                                                                                  | X  |    |
| Detalle de cualquier ingreso fallida desde el último ingreso                                                                                                                             |    | X  |

Tal como puede observarse en el Checklist anterior, para conectarse al sistema operativo del servidor, existe un procedimiento para el inicio de sesión. Es necesario destacar, que el mismo no muestra en pantalla ningún tipo de información relevante, ni muestra ningún tipo de identificador de sistema o de aplicación en pantalla, hasta que se completa el inicio de sesión. Por otro lado, no muestra ningún tipo de información de ayuda, ni valida ningún dato hasta que se completa el proceso de ingreso, y en el caso que se ingrese un usuario o contraseña inválido, no indica cual es la opción incorrecta. Al emplear el protocolo ssh para el inicio de sesión, la contraseña no es transmitida como texto limpio y la misma no se muestra en pantalla cuando es ingresada. Por otra parte, al completar el proceso de inicio de sesión, se muestra en pantalla cual fue el último ingreso exitoso, pero no se muestra ningún tipo de información acerca de ingresos previos fallidos. Finalmente, es necesario aclarar que se lleva registro de todos los intentos de inicio de sesión, tanto exitoso como fallido.

Cabe destacar que:

- No existe un límite de intentos de ingreso fallidos.
- No se establece un tiempo de retraso antes de permitir un nuevo intento de inicio de sesión, luego de un intento fallido.
- No envía ningún mensaje de alerta cuando alguien supera o alcanza el límite máximo de intentos permitidos.
- No se limita el tiempo máximo y mínimo para el procedimiento de ingreso al sistema.

#### 4.6.5.1.1 Cambios recomendados

Con el objetivo de cumplimentar las directrices establecidas en el presente control, recomendamos la implementación de un “*Controlador de Dominio*”, el cual permite centralizar la gestión de los usuarios y contraseñas de acceso a los sistemas operativos de las computadoras del Hospital. Puede emplearse, tanto la tecnología de la empresa “*Microsoft*”, para lo que es necesario adquirir las licencias correspondientes, como software de tipo “*open source*” (Es posible que, para este tipo de solución, no sea posible implementar todas las funcionalidades requeridas).

Será necesaria la creación de un usuario individual para cada empleado del Hospital, y un grupo de usuario por cada sector/programa del Hospital. Esto permite, no solo centralizar la gestión de los usuarios de los sistemas operativos, sino también establecer restricciones de acceso a las diversas funcionalidades y configuraciones de dichos sistemas. Es recomendable que los usuarios no dispongan de privilegios de administrador.

Se debe configurar adecuadamente el “*Controlador de Dominio*” para que:

- No se provea ningún tipo de ayuda para el inicio de sesión.
- Restringir de forma total el acceso a la información almacenada en las computadoras, hasta que se complete el procedimiento de inicio de sesión.
- No se indiquen que datos son erróneas durante un intento fallido de inicio de sesión.
- Se limiten el número de ingresos fallidos (Se recomiendan entre 4 y 10 intentos de sesión fallidos).
- Se registren los intentos fallidos y exitosos de inicio de sesión (Esto se logra activando, en el caso de los productos de “*Microsoft*”, la auditoria de eventos de inicio de sesión)

- Al alcanzar el número límite de ingresos fallidos, la cuenta implicada sea bloqueada y requiera la intervención del personal del sector de Sistemas Informáticos para su desbloqueo.
- Al bloquearse una cuenta, debido a que se superaron el número de intentos permitidos de inicio de sesión, se envíe una notificación al responsable de la seguridad de la información para que el mismo evalúe la situación.
- Al iniciar sesión en el sistema operativo, se muestre en pantalla la fecha del último inicio de sesión exitoso, la fecha del último ingreso fallido de sesión y el número de ingresos fallidos previos al actual inicio de sesión.

Es importante aclarar en este punto, que las contraseñas, por defecto, no son transmitidas a través de la red como texto plano, sino que, en base a la versión del Sistema Operativo del servidor, se emplea una técnica de cifrado determinada.

Por otro lado, es necesario configurar cada computadora del Hospital, para incluirla al dominio previamente mencionado. También es necesario habilitar el usuario “*Administrador*” en cada una de las mismas, de manera que se disponga de un usuario local con el cual pueda darse mantenimiento a la PC en caso que el sistema operativo no funcione adecuadamente; sin embargo, es necesario asignar una contraseña segura a dicho usuario, que solamente sea conocida por el personal del sector de Sistemas Informáticos. Por otro lado, es necesario cambiar la configuración de cada PC, para que las mismas no muestren los usuarios con los que se inició sesión anteriormente, y sea necesario ingresar tanto el usuario como la contraseña, de manera tal que se evite mostrar cualquier tipo de información relevante en la pantalla de inicio de sesión.

Para establecer una adecuada configuración que ayude a cumplimentar con los lineamientos propuestos por la NORMA ISO 27002:2008, se deben considerar también las configuraciones requeridas en “*Identificación y autenticación de usuarios*” (4.6.5.2.1), “*Sistema de administración de contraseñas*” (4.6.5.3.1), “*Uso de utilitarios de sistema*” (4.6.5.4.1), “*Expiración de la sesión*” (4.6.5.5.1), “*Limitaciones del tiempo de conexión*” (4.6.5.6.1). En este punto, también es posible, en el caso que se considere necesario, implementar la solución establecida en “*Revisiones técnicas de las aplicaciones luego de cambios en el sistema operativo*” (4.7.5.2.2), para gestionar las actualizaciones de los sistemas operativos en las terminales de los usuarios del Hospital.

Para poder implementar el “*Controlador de Dominio*” utilizando las herramientas Microsoft, se deberá, en primer lugar, adquirir las licencias de los sistemas operativos de las computadoras disponibles en la institución (aproximadamente 140), y, en segundo lugar, adquirir o montar un servidor que sea capaz (cumplir con los requerimientos del software) de soportar al “*Controlador de Dominio*”.

Finalmente, consideramos que, con las mejoras propuestas, se cumplirían con los puntos establecidos por el presente control.

#### 4.6.5.2 *Identificación y autenticación de usuarios*

##### **Control**

*“Se recomienda que todos los usuarios tengan un único identificador (Identificador de usuario) para su uso personal, y que se elija una técnica adecuada de autenticación para sustentar la identidad segura del usuario”<sup>145</sup>*

### **Relevamiento**

Con el objeto de examinar el cumplimiento del presente control en la organización, se realizó una entrevista al jefe del sector de sistemas informáticos, debido a que consideramos que la creación y distribución de usuarios para acceder a los sistemas operativos depende del sector previamente mencionado.

En base a lo establecido en el control *“Identificación y autenticación de usuarios”* de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:

- ¿Cada uno de los empleados del Hospital (incluido el personal del sector de Sistemas Informáticos) disponen de un usuario propio para acceder a los sistemas operativos instalados en las computadoras del Hospital?
- ¿Todos los empleados cuentan con cuentas privilegiadas?
- ¿Se emplean usuarios compartidos entre varios empleados? ¿Por qué razón se emplean? ¿Se encuentran debidamente identificados y autorizados por la gerencia?
- ¿Se emplean identificadores genéricos? ¿Estos usuarios disponen de un nivel de privilegios elevado? ¿Es necesario rastrear las acciones llevadas a cabo por dicho usuario?
- En caso de autenticación estricta ¿Se emplean métodos alternativos a las contraseñas (por ejemplo, “tokens”)? ¿Se combinan diferentes métodos de autenticación?

En base a la información obtenida durante la entrevista, realizada el día 15/03/2016, se procedió a completar el siguiente Checklist:

| Identificación y autenticación de usuarios                                                                    | Si | No |
|---------------------------------------------------------------------------------------------------------------|----|----|
| Cada usuario del hospital tiene asignado un identificador de usuario propio para acceder al sistema operativo |    | X  |
| Usuarios regulares NO tienen cuentas privilegiadas                                                            |    | X  |
| Se emplean identificadores compartidos de usuarios (grupos de usuarios)                                       |    | X  |
| La gerencia aprueba la creación y el uso de los identificadores compartidos                                   |    | X  |
| En caso de autenticación estricta, se emplean otros medios para verificar la identidad del usuario            |    | X  |
| En caso de autenticación estricta se combinan varios métodos de autenticación                                 |    | X  |

Tabla 4.6-16

Podemos ver en el Checklist anterior que, a pesar que existe un procedimiento para el inicio de sesión en el sistema operativo de la computadoras de tipo “cliente”, no se asigna un

<sup>145</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

usuario propio a cada empleado, sino que, en lugar de ello, se crea un usuario genérico en cada PC, y se le asigna una contraseña especial, la cual es común y conocida por todos los empleados de la Organización, o bien, por pedido expreso del jefe del sector/programa se le asigna una contraseña común únicamente a los empleados del sector/programa. Es necesario aclarar que dicho usuario tiene privilegios de administrador. Por estas razones, consideramos que el presente control no se cumplimenta adecuadamente.

#### 4.6.5.2.1 Cambios recomendados

Para cumplimentar los objetivos del presente control, es necesario ampliar ciertas configuraciones de la solución propuesta en **4.6.5.1.1**(Procedimientos seguros de inicio de sesión). En la misma se establece que debe otorgarse un usuario propio a cada usuario para acceder al sistema operativo y que, además, los mismos no pueden contar con privilegios de administrador.

Consideramos que deben crearse grupos de usuario para cada sector/programa del Hospital, y establecerse derechos de acceso y privilegios para cada grupo, para lo cual, es necesario realizar un análisis para determinar el nivel de acceso requerido por los usuarios del Hospital. Así mismo, deberán incluirse en estos grupos los usuarios correspondientes.

Por otra parte, no estimamos necesario el uso de identificadores compartidos, o el uso de medios de autenticación adicionales.

#### 4.6.5.3 Sistema de Administración de contraseñas

##### **Control**

*“Se recomienda que los sistemas que administran contraseñas sean interactivos y garanticen contraseñas de calidad.”<sup>146</sup>*

##### **Relevamiento**

Para verificar el cumplimiento del presente control dentro de la organización se procedió a realizar una entrevista al Jefe del Sector de Sistemas Informáticos, ya que consideramos que la administración de contraseñas de acceso a los sistemas operativos corresponde al sector previamente mencionado

Teniendo en cuenta lo establecido en el control “*Sistema de administración de contraseñas*” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:

- ¿Se dispone de un sistema para la administración de las contraseñas de usuario para acceder a los sistemas operativos?
- ¿Se emplean usuarios y contraseñas individuales?
- ¿Los usuarios tienen la opción de cambiar su contraseña de inicio al SO? ¿Se le muestran los errores en el caso que ingrese una nueva contraseña incorrecta?
- ¿Se impone el uso de contraseñas de calidad? ¿Qué requisitos deben cumplir las contraseñas?
- ¿Se impone el cambio de contraseña cada un cierto intervalo de tiempo?
- ¿Los usuarios deben cambiar la contraseña en su primer acceso?

---

<sup>146</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

- ¿Se mantiene un registro de contraseñas para evitar que reutilicen las mismas?
- ¿Se muestra la contraseña en pantalla?
- ¿Las contraseñas son almacenadas en archivos diferentes a los de los datos del sistema?
- ¿Las contraseñas se transmiten de forma protegida?

Conforme a los datos obtenidos durante la entrevista realizada al jefe del sector de sistemas informáticos, realizada el día 15/03/2016, se completó el siguiente Checklist:

| Sistema de administración de contraseñas                                                           | Si | No |
|----------------------------------------------------------------------------------------------------|----|----|
| El sistema de administración de contraseñas:                                                       |    |    |
| Impone el uso de identificación de usuario y contraseña individuales                               |    | X  |
| Permite que los usuarios seleccionen y cambien sus contraseñas                                     |    | X  |
| Incluye procedimientos de confirmación de contraseñas para contemplar errores mientras se escriben |    | X  |
| Impone la elección de contraseñas de calidad                                                       |    | X  |
| Impone cambios de contraseña                                                                       |    | X  |
| Obliga a los usuarios a cambiar la contraseña temporarias en su primer ingreso al sistema          |    | X  |
| Mantiene registro de contraseñas previas del usuario y evita la reutilización de las mismas        |    | X  |
| No muestra las contraseñas en pantalla cuando se las ingresa                                       |    | X  |
| Almacena en forma separada los archivos de contraseñas y los datos del sistema de aplicación       |    | X  |
| Almacena y transmite las contraseñas de forma segura                                               |    | X  |

Tabla 4.6-17

Tal como se establece en **4.6.5.2**(Identificación y autenticación de usuarios), en los sistemas operativos de los clientes se establece una contraseña común para toda la organización, o bien una contraseña común y conocida únicamente por los empleados del sector/programa en cuestión, por lo que consideramos que no se cumplen los puntos establecidos por el presente control.

#### 4.6.5.3.1 Cambios recomendados

Con el propósito de cumplir adecuadamente con los puntos previamente mencionados en el presente control, sugerimos la implementación de la solución propuesta en **4.6.5.1.1**(Procedimientos seguros de inicio de sesión), ya que, en la misma se establece el uso de usuarios y contraseñas individuales. Por otra parte, el “Controlador de Dominio” permite a los usuarios establecer y cambiar sus contraseñas. Es necesario configurar el “Controlador de Dominio” para:

- Imponer el uso de contraseñas de calidad (es recomendable que se utilicen contraseñas con 8 caracteres mínimo, que incluyen un número, una letra y un carácter especial).

- Imponer el cambio de contraseñas cada un determinado período de tiempo. En el caso que se empleen contraseñas de calidad, recomendamos que el período establecido sea prolongado (Por ejemplo, una o dos veces al año).
- Mantener un registro de las contraseñas antiguas para evitar la reusabilidad de las mismas.

Es necesario aclarar que, por defecto, las contraseñas se transmiten de forma segura y las mismas no se muestran en pantalla al ser ingresadas.

Finalmente, recomendamos que el registro de nuevos usuarios en el “Controlador de Dominio” se realice en paralelo con el registro de nuevo usuarios del sistema, siguiendo el procedimiento establecido en 4.6.2.1.1(Registro de usuarios).

#### 4.6.5.4 Uso de utilitarios de sistema

##### Control

*“Se recomienda que el uso de programas utilitarios que pudiesen ser capaces de pasar por alto los controles de las aplicaciones o del sistema esté restringido y controlado de cerca”<sup>147</sup>*

##### Relevamiento

Con el fin de corroborar el cumplimiento del presente control en el hospital se mantuvo una entrevista con el jefe del sector de sistemas informáticos, debido a que consideramos que el control de los sistemas utilitarios es responsabilidad de dicho sector.

Durante la entrevista se realizaron las siguientes preguntas, en base a lo establecido en el control “Uso de utilitarios de sistema” de la norma IRAM-ISO/IEC 27002:2008:

- ¿Qué sistemas utilitarios se emplean en la Organización?
- ¿Existen procedimientos que permiten controlar el uso de los utilitarios del sistema?  
¿Qué controles se establecen sobre los mismos?
- ¿Se limita el uso de estos sistemas a un pequeño número de usuarios de confianza?
- ¿Se limita la disponibilidad de los utilitarios, por ejemplo, tras un determinado tiempo de uso?
- ¿Se establecen niveles de seguridad para los utilitarios?
- ¿Se elimina o deshabilita todo aquel utilitario innecesario?

En base a la información obtenida durante la entrevista, realizada el día 15/03/2016, se procedió a completar el siguiente Checklist:

| Uso de los utilitarios del sistema                                                                  | Si | No |
|-----------------------------------------------------------------------------------------------------|----|----|
| Existen procedimientos que permiten identificar, autenticar y autorizar sistemas utilitarios        |    | X  |
| Se limita el uso de sistemas utilitarios a un número reducido y controlado de usuarios de confianza |    | X  |
| Se limita la disponibilidad de sistemas utilitarios                                                 |    | X  |

<sup>147</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

|                                                                           |  |   |
|---------------------------------------------------------------------------|--|---|
| Se realiza el registro de todo uso de los sistemas utilitarios de sistema |  | X |
| Se definen y documentan los niveles de seguridad para los utilitarios     |  | X |
| Se desactiva o elimina todo software innecesario                          |  | X |

Tabla 4.6-18

Podemos visualizar en el Checklist anterior que no se disponen de procedimientos que permiten identificar, autenticar y autorizar sistemas utilitarios, y cabe destacar que no se realiza ningún tipo de control acerca del uso de los sistemas utilitarios, por lo que no se cumplimentan ninguno de los puntos establecidos por el presente control.

Cabe destacar en este punto que entre los utilitarios empleados dentro de la organización encontramos:

- Navegadores de Internet.
- Hojas de Cálculo.
- Procesadores de Texto.

#### 4.6.5.4.1 Cambios Recomendados

Para lograr el cumplimiento de lo establecido por el presente control, proponemos que se configure una “lista blanca”, ya sea en el “Controlador de Dominio” propuesto en **4.6.5.1.1**(Procedimientos seguros de inicio de sesión), o bien que sea configurada por separado en cada PC del Hospital. Esta herramienta permite definir un conjunto de aplicaciones que el usuario es capaz de ejecutar en la computadora, logrando de esta manera limitar el uso de los utilitarios del sistema, habilitando los mismos únicamente a aquellas personas que se encuentran autorizadas a ejecutar los mismos. Recomendamos la implementación de esta herramienta a través del “Controlador de Dominio”, a través de la aplicación “AppLocker”, ya que, a través de la misma, es posible mantener un registro del nivel de acceso de cada usuario para cada uno de los sistemas utilitarios, y mantener los programas innecesarios deshabilitados (al no permitir su ejecución). También, es conveniente que se establezcan y documenten una serie de reglas, procedimientos o directrices para identificar, autenticar y autorizar el uso de los sistemas utilitarios, las cuales deben ser establecidas por el Comité de la Seguridad de la Información (ver **4.2.1.2.1**(Coordinación de la Seguridad de la Información)).

Por otra parte, a través de la solución propuesta en **4.3.1.1**(Inventario de Activos), es posible mantener un registro de todos los sistemas utilitarios.

Finalmente, para llevar registro del uso de los utilitarios, es necesario habilitar la Auditoría de Creación de Procesos (“*Audit Process Creation*”) y la Auditoría de Terminación de Procesos (“*Audit Process Termination*”). Es recomendable habilitar dichas opciones desde el “Controlador de Dominio”, ya que, de esta manera, no es necesario configurar cada terminal por separado.

Es importante considerar las recomendaciones establecidas en **4.6.6.1.1**(Restricción de acceso a la información).

#### 4.6.5.5 Expiración de la sesión

##### **Control**

*“Se recomienda que las sesiones inactivas se cierren luego de un período definido de inactividad”<sup>148</sup>*

##### **Relevamiento**

Con el objeto de examinar el cumplimiento del presente control en la organización, se procedió a verificar en el lugar de trabajo, con la debida autorización del jefe de Sistemas Informáticos y el jefe del sector/programa involucrado, la configuración de la suspensión de los equipos (PCs de usuarios). Se comprobó si en la configuración energía de la computadora, se establecía un tiempo de inactividad tal el cual se suspendía o no el equipo. A continuación, se muestran los resultados obtenidos:

| Maquina | Sector      | ¿El equipo se suspende tras un determinado tiempo de inactividad? |
|---------|-------------|-------------------------------------------------------------------|
| 01      | Informática | No                                                                |
| 02      | Personal    | No                                                                |
| 03      | Estadística | No                                                                |
| 04      | Estadística | No                                                                |
| 05      | Estadística | Si (30 min)                                                       |
| 06      | Estadística | No                                                                |
| 07      | Estadística | No                                                                |
| 08      | RRHH        | Si (30 min)                                                       |
| 09      | RRHH        | Si (30 min)                                                       |
| 10      | Informática | Si (15 min)                                                       |

Tabla 4.6-19

Como puede observarse, el 40% de las computadoras se suspende tras un determinado tiempo, mientras que el resto no lo hace nunca.

<sup>148</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

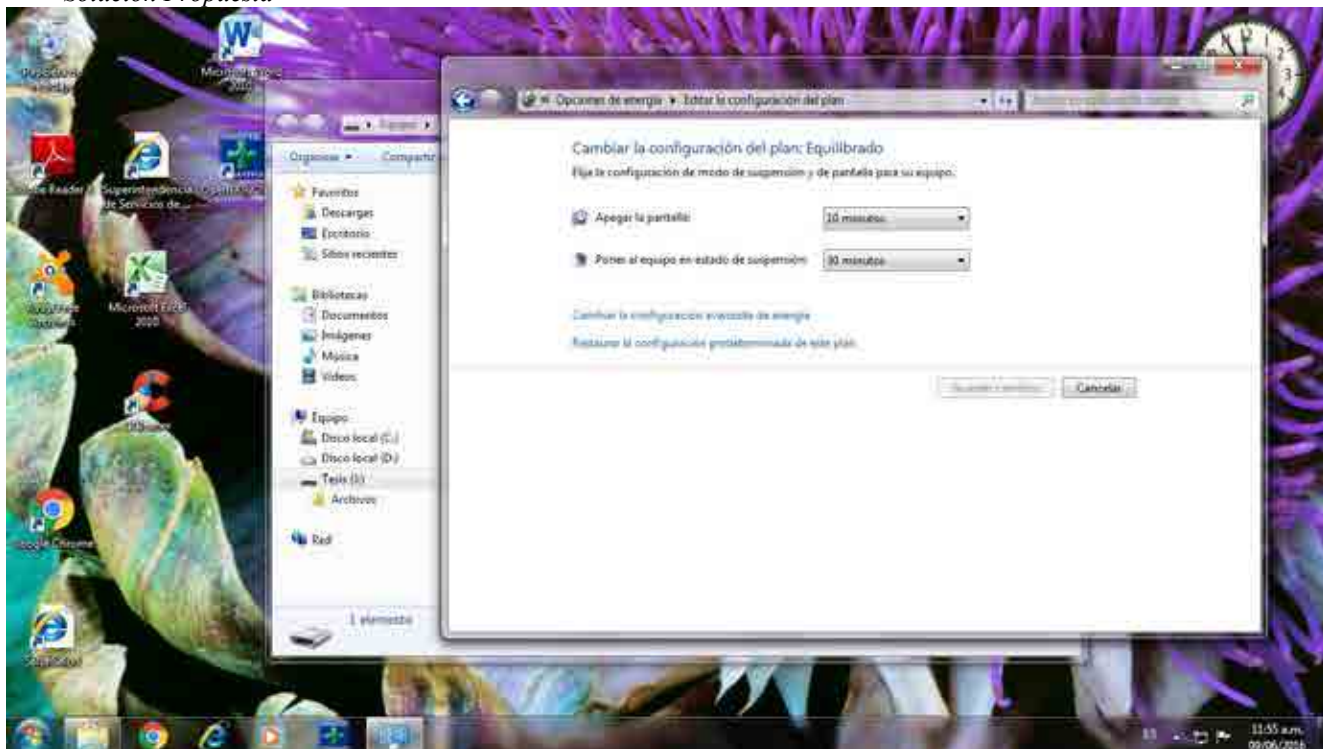


Ilustración 4.6-8

En la imagen anterior podemos apreciar que el tiempo de suspensión es de 30 minutos.

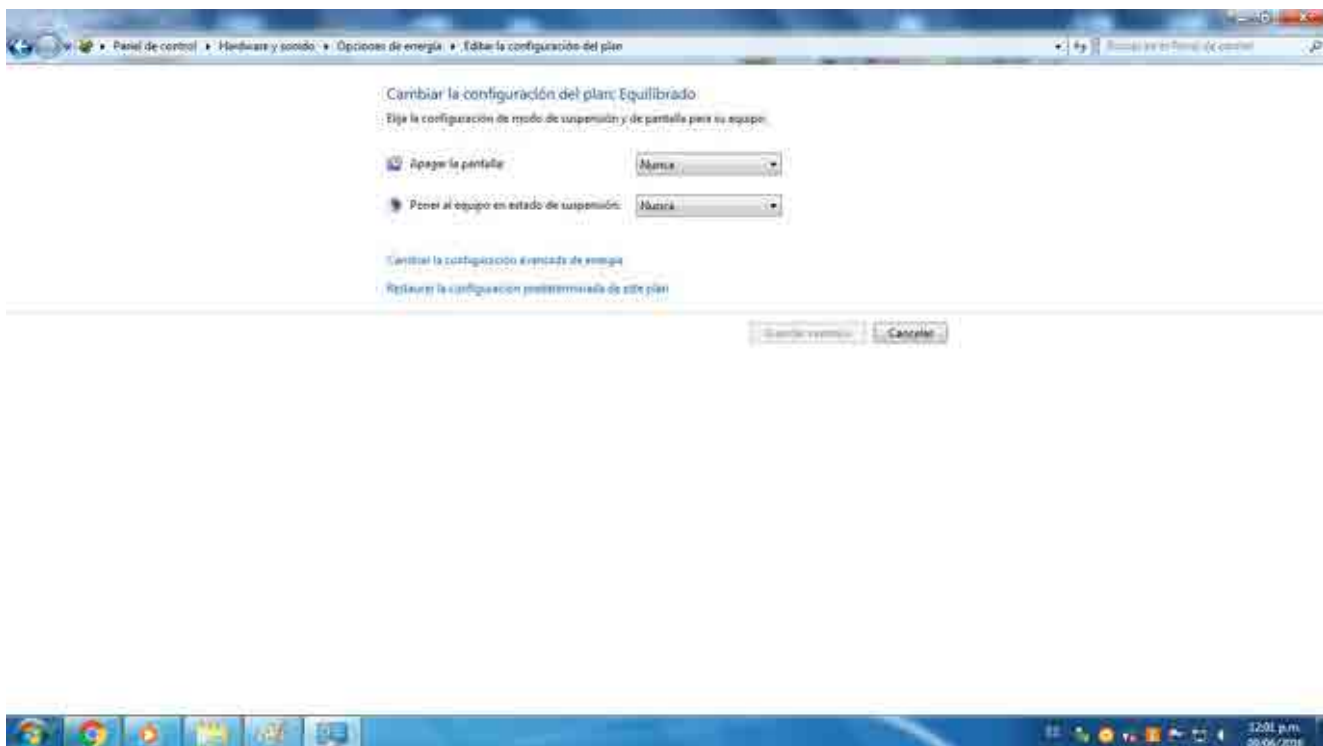


Ilustración 4.6-9

En la imagen anterior podemos apreciar que el equipo no se suspende nunca.

Conforme a los datos obtenidos durante la entrevista realizada el día 15/03/2016, se completó el siguiente Checklist:

*Yustman, Mauricio Ezequiel*

*Pérez Osán, Fernando Javier*

| Expiración de la Sesión                                                                                                                                                        | Si | No |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|
| La sesión del sistema operativo expira tras un tiempo determinado de inactividad                                                                                               |    | X  |
| Al expirar la sesión del sistema operativo, expira la sesión de la red                                                                                                         |    | X  |
| Al expirar la sesión del sistema operativo, expira la sesión de las aplicaciones                                                                                               |    | X  |
| El lapso de tiempo de inactividad antes de que expire la sesión se define de acuerdo a los riesgos del área y a la clasificación de la información que es manejada en la misma |    | X  |

Tabla 4.6-20

Como puede verse en el Checklist anterior, la gran mayoría de las computadoras de los usuarios no se encuentran configuradas para que, luego de un determinado tiempo de inactividad, expire la sesión, y por lo tanto no se cumplen con ninguno de los puntos establecidos en el presente control. (Considerando que durante el relevamiento solo el 40% de las máquinas estaba adecuadamente configurada.)

#### 4.6.5.5.1 Cambios Recomendados

Consideramos que, para cumplir adecuadamente con lo establecido en el presente control, se configure en el “Controlador de Dominio”, mencionado 4.6.5.1.1 (Procedimientos seguros de inicio de sesión), la expiración de la sesión de los usuarios tras un determinado tiempo de inactividad. Sin embargo, debido a que la autenticación de los usuarios debe realizarse en el Servidor en el que se encuentra instalado el “Controlador de Dominio”, sugerimos que no expire la sesión de la red. Por otro lado, recomendamos que, en base a los riesgos de cada sector/programa y a la sensibilidad de la información manejada en la misma, se establezca tiempos tras los cuales:

- Se bloquee la pantalla del Sistema Operativo: el tiempo para el bloqueo de la pantalla debe ser menor que el de expiración de la sesión. Permite que, tras un corto período de inactividad, sea necesario ingresar el usuario y la contraseña para continuar con el trabajo. Es necesario aclarar que, con el bloqueo de pantalla, no se cierra ninguna aplicación activa, sin embargo, es necesario ingresar las credenciales del usuario para continuar con su uso. Tiene como ventajas la protección de la información almacenada, cuando la terminal se encuentra desatendida, y que además permite retomar fácilmente el trabajo que se encontraba realizando el usuario sin generar ningún tipo de pérdidas.
- Expire la sesión del Sistema Operativo: Se recomienda que, en el caso que se establezca un tiempo para el bloqueo de la pantalla, se defina un tiempo prolongado antes que se genere el cierre de sesión. Es necesario aclarar que cuando se produce el mismo, todas las aplicaciones se cierran automáticamente, por lo que es posible que los usuarios pierdan una parte del trabajo que se encontraban realizando.

Cabe destacar que, es posible establecer esta configuración de manera local, sin embargo, es recomendable la implementación y correcta configuración del “Controlador de Dominio”, propuesto en 4.6.5.1.1 (Procedimientos seguros de inicio de sesión), de manera que sea posible mantener la gestión de la seguridad de los sistemas operativos de manera centralizada.

#### **Control**

*“Se recomienda que se utilicen restricciones acerca del tiempo de conexión para brindar seguridad adicional a las aplicaciones de alto riesgo”<sup>149</sup>*

#### **Relevamiento**

Con el objeto de examinar el cumplimiento del presente control en la organización, se realizó una entrevista al jefe del sector de sistemas informáticos, debido a que consideramos que la responsabilidad de definir una limitación del tiempo de conexión a los sistemas sensibles pertenece al sector previamente mencionado

En base a lo establecido en el control *“Limitaciones del tiempo de conexión”* de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:

- ¿Se establece alguna limitación del tiempo de conexión para los sistemas internos del Hospital? ¿Qué restricciones se aplican? ¿Por qué?
- En locaciones de alto riesgo, por ejemplo, en áreas públicas del Hospital ¿Se establece algún tipo de limitación en el tiempo de conexión?

En base a la información obtenida durante la entrevista, realizada el día 15/03/2016, se procedió a completar el siguiente Checklist:

| Limitaciones del tiempo de conexión                                                                                    | Si | No |
|------------------------------------------------------------------------------------------------------------------------|----|----|
| Existen restricciones especiales para aquellas aplicaciones sensibles o que se encuentran en locaciones de alto riesgo |    | X  |

Tabla 4.6-21

Como podemos ver en el Checklist anterior, no se aplican restricciones especiales que limiten el tiempo de conexión para las aplicaciones del Hospital, y en consecuencia no se cumplimenta lo establecido en el presente control.

Consideramos que existe una ubicación de alto riesgo dentro del Hospital, la cual es el área de atención al público. Sin embargo, es necesario aclarar que no se limita el tiempo de conexión de la aplicación de gestión Hospitalaria ni de la sesión del sistema operativo.

##### 4.6.5.6.1 Cambios Recomendados

Proponemos que, al momento de establecer el tiempo tras el cual se produce el bloqueo de pantalla y la finalización de la sesión, tal como se menciona en **4.6.5.5.1** (Expiración de la Sesión), se consideren tiempos más reducidos que los propuestos para terminales ubicadas en otros puntos del Hospital. En caso que, en el futuro se ubiquen terminales en otras ubicaciones de alto riesgo, se evalúe la situación y se establezcan los controles necesarios.

#### 4.6.6 Control de acceso a las aplicaciones y a la información

*“Objetivo: Prevenir el acceso no autorizado a la información contenida en los sistemas de aplicación.”*

<sup>149</sup> IRAM-ISO/IEC 27002:2008  
 Yustman, Mauricio Ezequiel

*Se recomienda que se utilicen los recursos de seguridad para limitar tanto el acceso a los sistemas de aplicación como a su estructura interna.*

*Se recomienda que se limite el acceso lógico al software de aplicación y a la información solo a los usuarios autorizados. Es conveniente que los sistemas de aplicación:*

- a) Controles el acceso de usuarios a la información y a las funciones de los sistemas de aplicación, de acuerdo con la política de control de acceso definida.*
- b) Brinden protección contra el acceso no autorizado de cualquier utilitario, software del sistema operativo y software malicioso que tengan la capacidad de pasar por alto los controles de los sistemas de las aplicaciones.*
- c) No comprometan otros sistemas con los que se comparten recursos de información.”<sup>150</sup>*

#### 4.6.6.1 Restricción de acceso a la información

##### **Control**

*“Se recomienda que se restrinja el acceso a la información y a las funciones de los sistemas de aplicación a los usuarios y al personal de soporte, de acuerdo con una política de control de acceso definida.”<sup>151</sup>*

##### **Relevamiento**

Con el fin de corroborar el cumplimiento de los lineamientos propuestos por el control bajo estudio, se realizaron las siguientes actividades:

- Observación: Se solicitó al administrador del sistema, la creación de un usuario con un número limitado de funcionalidades. Asimismo, se visualizó las opciones que poseía otro usuario con más funcionalidades permitidas. A continuación, se muestran dos imágenes correspondientes a cada usuario:

A. Usuario con más funcionalidades permitidas.



Ilustración 4.6-10

<sup>150</sup> IRAM-ISO/IEC 27002:2008

<sup>151</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

## B. Usuario con funcionalidades limitadas

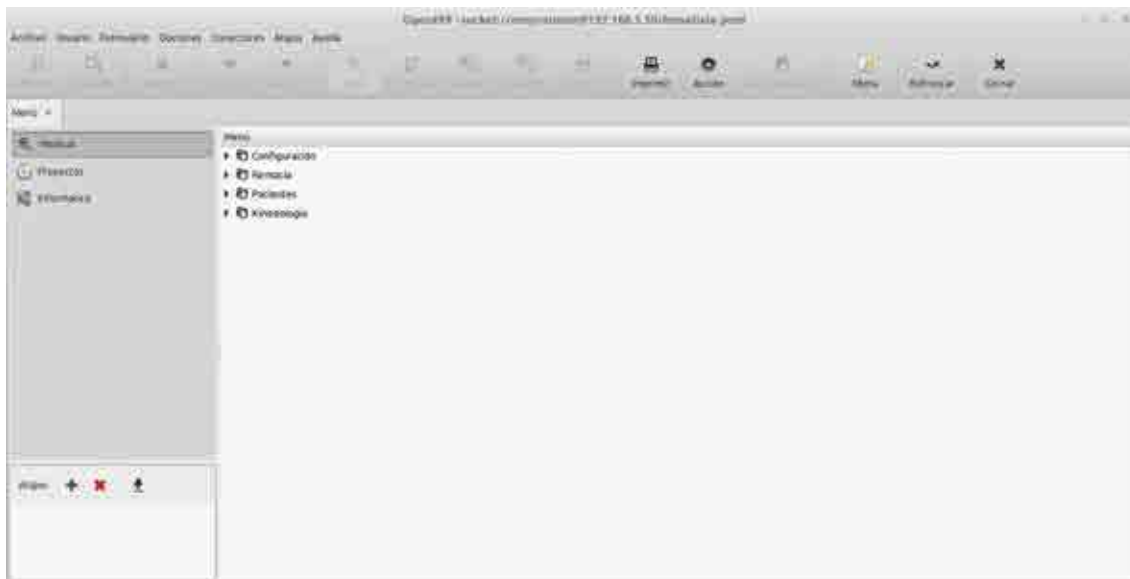


Ilustración 4.6-11

- Entrevista al Jefe del Sector de Sistemas Informáticos. Teniendo en cuenta lo establecido en el control “*Restricción de acceso a la información*” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:
  - ¿El sistema de gestión Hospitalario establece restricciones de acceso para cada uno de los módulos en función del usuario que ingresa al sistema?
  - ¿Se dispone de un menú principal que permite acceder a los diversos módulos y funcionalidades del sistema? ¿Se le permite visualizar a los usuarios aquellas opciones que les fueron habilitadas por el administrador del sistema?
  - ¿Se establecen derechos de acceso para cada usuario, por ejemplo, para lectura, escritura y eliminación?
  - ¿Se establecen derechos de acceso para otras aplicaciones?

Conforme a los datos obtenidos durante la entrevista realizada al jefe del sector de sistemas informáticos, realizada el día 15/03/2016, se completó el siguiente Checklist:

| Restricción de acceso a la información                                                                                                      | Si | No |
|---------------------------------------------------------------------------------------------------------------------------------------------|----|----|
| Se establecen restricciones de acceso a las diversas funcionalidades o módulos del sistema ERP del Hospital                                 | X  |    |
| El sistema ERP proporciona un menú principal que permite controlar el acceso a los diversos módulos del sistema                             | X  |    |
| Un usuario solamente es capaz de visualizar en dicho menú aquellas opciones que el administrador del sistema le ha autorizado para ingresar | X  |    |
| Se establece derechos de acceso para cada usuario (Por ejemplo, para lectura, escritura, eliminación)                                       | X  |    |

|                                                          |  |   |
|----------------------------------------------------------|--|---|
| Se establecen derechos de acceso para otras aplicaciones |  | X |
|----------------------------------------------------------|--|---|

Tabla 4.6-22

Como puede verse en el Checklist anterior, existen restricciones de acceso a los módulos del sistema ERP, que dependen del rol del usuario conectado, el cual es asignado por el personal del área de sistemas informáticos, en base al cargo del empleado y al sector o programa en el que trabaja. Dependiendo del rol anteriormente mencionado, se habilitan o deshabilitan en el menú principal del sistema el acceso a los diversos módulos del sistema, y se define para cada una de las funcionalidades, si el usuario dispone de privilegios para consultar, editar o eliminar la información a la que accede.

Por otro lado, es necesario destacar que no se establecen restricciones de acceso a otras aplicaciones, ya sean utilitarios, o bien sistemas independientes mencionados en 4.5.8.5(Sistema de información del negocio). Sin embargo, estos se encuentran instalados en aquellas computadoras en las que son requeridas, por lo que el acceso a estas aplicaciones se limitaría al personal del sector o programa. A pesar de esto, consideramos que no se cumplimenta de manera adecuada con el último punto del presente control.

#### 4.6.6.1.1 Cambios Recomendados

Debido a que no se establecen restricciones de acceso a los sistemas utilitarios o a los sistemas independientes mencionados en 4.5.8.5(Sistema de información del negocio), es recomendable implementar la solución propuesta en 4.6.5.4.1(Uso de utilitarios de sistema), e incluir dentro de la “lista blanca” mencionada, los sistemas independientes mencionados para aquellos usuarios autorizados.

#### 4.6.6.2 Aislamiento de sistemas sensibles

##### **Control**

*“Se recomienda que los sistemas sensibles se encuentren en un ambiente informático dedicado (aislado)”<sup>152</sup>*

##### **Relevamiento**

Con el fin de corroborar el cumplimiento del presente control en el hospital se mantuvo una entrevista con el jefe del sector de sistemas informáticos, ya que consideramos que el aislamiento de sistemas sensibles es responsabilidad del sector previamente mencionado.

Durante la entrevista se realizaron las siguientes preguntas, en base a lo establecido en el control “Aislamiento de sistemas sensibles” de la norma IRAM-ISO/IEC 27002:2008:

- ¿Se identifica la sensibilidad de cada una de las aplicaciones existentes dentro de la organización?
- ¿Los sistemas sensibles se ejecutan en computadoras dedicadas cuando es posible? Cuando no es posible, ¿Se comparten recursos únicamente con aplicaciones confiables?
- Para los sistemas sensibles que se ejecutan en entornos compartidos, ¿Se identifican y aceptan los sistemas con los que se comparten recursos? ¿Se identifican y aceptan los riesgos asociados?

<sup>152</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

En base a la información obtenida durante la entrevista, realizada el día 15/03/2016, se procedió a completar el siguiente Checklist:

| Aislamiento de Sistemas Sensibles                                                                                                                                               | Si | No |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|
| La sensibilidad de los sistemas de aplicación están claramente identificadas y documentadas                                                                                     |    | X  |
| Para los sistemas sensibles que se ejecutan en entornos compartidos, previamente el propietario del mismo identifica y acepta los recursos a ser compartidos                    |    | X  |
| Para los sistemas sensibles que se ejecutan en entornos compartidos, previamente el propietario del mismo identifica los riesgos que involucra el ambiente en el que se ejecuta |    | X  |
| Los sistemas sensibles se ejecutan en computadoras dedicadas                                                                                                                    |    | X  |
| Los sistemas sensibles solamente comparten recursos con aplicaciones confiables                                                                                                 |    | X  |

Tabla 4.6-23

Podemos apreciar en el Checklist anterior que no se identifica la sensibilidad de las aplicaciones dentro de la organización. Se consultó además acerca de la existencia de aplicaciones especiales que se encuentren aisladas, o sobre las que se apliquen controles o se tengan consideraciones especiales, sin embargo, el personal del sector de Sistemas Informáticos indicó que no existen programas sobre los que, por su alta sensibilidad, se apliquen controles especiales o que se ejecuten de forma aislada a los restantes. Por estas razones, consideramos que no se cumplimentan los puntos establecidos por el presente control.

#### 4.6.6.2.1 Consideraciones de control

Para aquellos activos de software con una alta sensibilidad, y en caso de ser posible, se recomienda que se configure una computadora dedicada para alojar este tipo de software. Es necesario tomar las precauciones correspondientes al momento de configurar la computadora previamente mencionada, de manera que se logren evitar accesos no autorizados, o la ejecución de software no autorizado en la misma. Por otro lado, en el caso que el software sensible deba ejecutarse en entornos compartidos (al requerir datos de otros entornos o programas), es necesario identificar y aceptar tanto los datos compartidos como los riesgos relacionados. Finalmente, se recomienda que el software sensible únicamente comparta sus datos con aplicaciones confiables.

#### 4.6.7 Computación móvil y teletrabajo

*“Objetivo: Garantizar la seguridad de la información mientras se utilizan dispositivos de computación móvil e instalaciones de teletrabajo.*

*Se recomienda que la protección requerida sea proporcional a los riesgos que originan estas formas específicas de trabajo. Es conveniente que, mientras se utiliza computación móvil en un ambiente desprotegido, se consideren los riesgos que esto implica y se implemente la protección adecuada. En el caso del teletrabajo, se recomienda que la organización*

*implemente protección en el sitio remoto de teletrabajo y garantice que se toman las medidas adecuadas para este tipo de trabajo.”<sup>153</sup>*

#### 4.6.7.1 Computación y comunicaciones móviles

##### **Control**

*“Se recomienda que se establezca una política formal y que se adopten medidas de seguridad adecuadas para protegerse contra los riesgos del uso de dispositivos de computación e instalaciones de comunicaciones móviles.”<sup>154</sup>*

##### **Relevamiento**

Con el propósito de examinar el cumplimiento del presente control, se realizó una entrevista al Jefe del Sector de Sistemas Informáticos, dado que, es este sector el encargado de configurar los dispositivos móviles otorgados por la organización a sus empleados.

De acuerdo a lo establecido en el control “*Computación y comunicaciones móviles*” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:

- ¿Existen políticas o reglamentos documentados acerca de la computación móvil?
- ¿Cuáles son los puntos contemplados por estas políticas o reglamentos?
- ¿Se toman recaudos para el uso de estos dispositivos en lugares públicos o fuera de las áreas protegidas de la organización?
- ¿Se toman recaudos para evitar el acceso no autorizado a estos dispositivos?
- ¿Los dispositivos móviles se encuentran protegidos por un Antivirus? ¿Se actualiza regularmente?
- ¿Se realizan copias de seguridad de la información almacenada en los dispositivos móviles? ¿Existe una forma sencilla de realizar estas copias de seguridad? ¿Dichas copias se encuentran almacenadas de manera adecuada y protegidas contra amenazas?
- ¿Se permite el acceso remoto al equipamiento de la organización desde la red pública? ¿Se emplea un método seguro de autenticación para el ingreso remoto?
- ¿Los dispositivos móviles cuentan con mecanismos para protegerlos frente a hurtos?
- Cuando los dispositivos no se encuentran en uso ¿Se los almacena de manera adecuada, en un lugar seguro bajo llave?
- ¿Se brinda algún tipo de capacitación especial a los usuarios que hacen uso de los dispositivos móviles? ¿Cuál es el contenido de esta capacitación?

Conforme a los datos obtenidos durante la entrevista realizada el día 15/03/2016, se completaron los siguientes Checklist:

| Computación y Comunicaciones móviles                                                   | Si | No |
|----------------------------------------------------------------------------------------|----|----|
| Existen políticas o reglamentos claramente documentados acerca de la computación móvil |    | X  |
| La política de computación móvil incluye requerimientos para:                          |    |    |

<sup>153</sup> IRAM-ISO/IEC 27002:2008

<sup>154</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

|                                                                                                                                                                                                                                                   |   |   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|
| La Protección Física                                                                                                                                                                                                                              |   | X |
| Técnicas Criptográficas                                                                                                                                                                                                                           |   | X |
| Copias de Respaldo                                                                                                                                                                                                                                |   | X |
| Protección de Virus                                                                                                                                                                                                                               |   | X |
| Se toman recaudos o bien se restringe el uso de dispositivos informáticos en lugares públicos o bien en áreas no protegidas de la organización.                                                                                                   |   | X |
| Se toman recaudos para evitar el acceso no autorizado a los dispositivos móviles                                                                                                                                                                  | X |   |
| Se toman recaudos para evitar la divulgación no autorizada de información almacenada y procesada en los dispositivos móviles                                                                                                                      |   | X |
| Los dispositivos móviles se encuentran adecuadamente protegidos por un antivirus                                                                                                                                                                  | X |   |
| El antivirus de los dispositivos móviles se actualiza regularmente                                                                                                                                                                                | X |   |
| Se realizan copias de seguridad de la información almacenada en los dispositivos móviles de la organización                                                                                                                                       |   | X |
| Las copias de seguridad pueden ser realizadas de forma rápida y sencilla                                                                                                                                                                          |   | X |
| Las copias de seguridad se encuentran debidamente almacenadas y protegidas contra amenazas                                                                                                                                                        |   | X |
| Se permite el acceso remoto al equipamiento de la organización desde la red pública                                                                                                                                                               |   | X |
| El acceso remoto al equipamiento de la organización solamente es posible a través de un proceso de autenticación exitoso                                                                                                                          |   | X |
| Los dispositivos móviles cuentan con mecanismos que permiten protegerlos frente al hurto                                                                                                                                                          |   | X |
| Cuando los dispositivos no se encuentran en uso, los mismos se encuentran debidamente almacenados y resguardados bajo llave, o bien a través de otro tipo de cerradura                                                                            | X |   |
| Se brinda capacitación especial a los usuarios que hacen uso de dispositivos móviles, acerca de los riesgos adicionales generados por la forma de trabajo de los mismos, y las recomendaciones o controles especiales que son necesarios aplicar. |   | X |

Tabla 4.6-24

Como podemos ver en el Checklist anterior, no existen reglas o políticas documentadas acerca de la computación móvil, sin embargo, se toman ciertos recaudos para proteger los dispositivos móviles que son propiedad de la organización. Es necesario aclarar que actualmente, el Hospital cuenta con una notebook, la cual puede ser solicitada por los empleados de la organización. Por otro lado, el sector de Patrimonio distribuye celulares a

aquellos empleados que lo solicitan, sin embargo, es necesario recalcar que dichos dispositivos son únicamente teléfonos celulares y no teléfonos inteligentes o “*Smartphones*”, por lo que la información almacenada dentro de los mismos es mínima, y no fueron considerados dentro del análisis del presente control.

Entre los recaudos o medidas especiales para proteger el dispositivo móvil con el que cuenta la organización, y la información almacenada en el mismo, encontramos:

- Se crea un usuario para cada empleado que solicita el dispositivo móvil. Dichos usuarios no disponen de privilegios de administrador, por lo que no es posible acceder a la información perteneciente a un usuario diferente.
- El dispositivo cuenta con un antivirus que es actualizado regularmente.
- Cuando el dispositivo no se encuentra en uso, el mismo se encuentra almacenado en un armario bajo llave.

Finalmente, es necesario aclarar que, el acceso remoto a los dispositivos de la organización no se encuentra permitido.

#### 4.6.7.1.1 Cambios Recomendados

En primer lugar, para cumplir adecuadamente con los puntos establecidos por el control, es necesario elaborar una política para el uso adecuado de los dispositivos móviles del Hospital. La misma, debe ser elaborada por el comité de seguridad de la información y aprobada por la gerencia del Hospital. Consideramos que los temas mínimos a desarrollar en la política anteriormente mencionada son los siguientes:

- Protección Física: se deben definir las consideraciones o reglas básicas a tener en cuenta para proteger la integridad de los dispositivos físicos bajo el cuidado del usuario (Por ejemplo, nunca perder de vista el dispositivo, ya que se corre el riesgo de sufrir un robo o hurto del mismo).
- Técnicas Criptográficas: sugerimos que se establezcan pautas para el uso de programas que permitan cifrar la información de alta sensibilidad almacenada en los dispositivos móviles, de manera que, solamente aquellas personas que se encuentren autorizadas tengan acceso a la misma.
- Copias de Respaldo: recomendamos que se establezca la obligación de realizar copias de seguridad de la información almacenada en los dispositivos móviles cada intervalo regular de tiempo.
- Protección de virus: debe establecerse la manera y las herramientas a emplear para proteger los dispositivos móviles de los virus informáticos.

Proponemos tomar como modelo de política la “*Guía para proteger y usar de forma segura su móvil*”, publicada por el “*Instituto Nacional de Tecnologías de la Comunicación*” (INTECO), que se encuentra disponible a partir del siguiente link:

<https://www.incibe.es/extfrontinteco/img/File/intecocert/Proteccion/usoseguromoviles.pdf>  
(vigencia: 02/06/2016)

Por otra parte, para proteger el dispositivo cuando el mismo se conecta a las redes públicas, sugerimos configurar el dispositivo de la siguiente manera:

- Deshabilitar el uso compartido para redes públicas, de manera tal que otros dispositivos conectados a la red no sean capaces de detectar el mismo.
- Activar el firewall del dispositivo, en caso que el Sistema Operativo disponga de uno, o bien instalar un firewall básico en el mismo.
- En caso de ser posible, hacer uso de un VPN (Virtual Private Network), ya que, el emplear este tipo de software, la información es cifrada antes de transmitirse a través de la red.

En cuanto a los recaudos a tomar para evitar la divulgación de información sensible almacenada en el dispositivo móvil, proponemos que se empleen programas de cifrado de datos, de manera que únicamente las personas autorizadas sean capaces de visualizar dicha información. Es necesario que, en base a las necesidades de la organización, el personal del sector de Sistemas Informáticos seleccione una aplicación para el cifrado de datos y capacite a los usuarios que soliciten los dispositivos móviles acerca de su uso.

Finalmente, es recomendable que se capacite a los usuarios acerca de los riesgos asociados al uso de los dispositivos móviles, sobre las políticas anteriormente mencionadas, la importancia y la forma de realizar copias de seguridad, y sobre el uso de los programas para el cifrado de datos. Sugerimos que estos temas sean incluidos en los temas de la capacitación de los empleados, a los mencionados en **4.4.2.2.1**(Concientización, Educación y Entrenamiento en Seguridad de la Información).

#### 4.6.7.2 Teletrabajo

##### **Control**

*“Se recomienda que se desarrolle e implemente una política, planes y procedimientos operacionales para las actividades de teletrabajo.”<sup>155</sup>*

##### **Relevamiento**

Se consultó si el teletrabajo es aplicado en la institución y se determinó que el mismo no es empleado, ya que todos los empleados realizan su trabajo de manera presencial. Es por esta razón que el presente control no fue analizado en el proyecto de grado desarrollado.

#### 4.6.8 Plan de trabajo

##### 4.6.8.1 Requisitos previos

Serán requisitos previos para la implementación de las soluciones propuestas

- La existencia del rol de responsable de seguridad de la información dentro de la institución (tal como se menciona en **4.1.1.3**(política de seguridad)).
- La existencia del Comité de Seguridad de la Información (tal como se menciona en **4.2.1.2.1**(Coordinación de la Seguridad)).
- La existencia de una Política de Seguridad en el Hospital (ver **4.1.1.3**(política de seguridad)).

##### 4.6.8.2 WBS (Estructura de Desglose de Trabajo)

A continuación, se establecen las actividades a llevar a cabo para implementar las soluciones propuestas en el presente control.

---

<sup>155</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

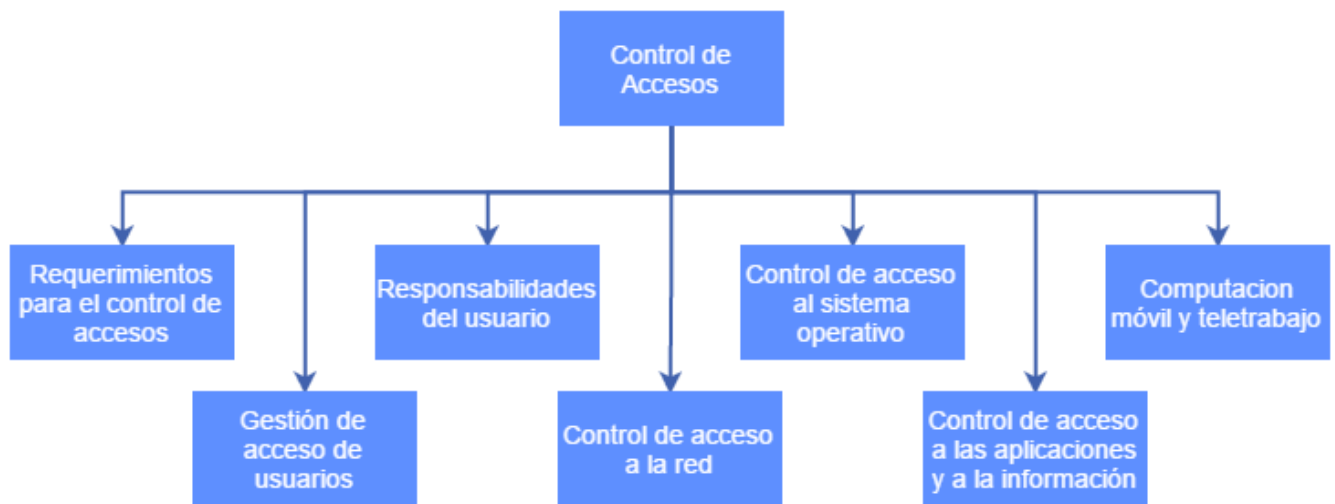


Ilustración 4.6-12

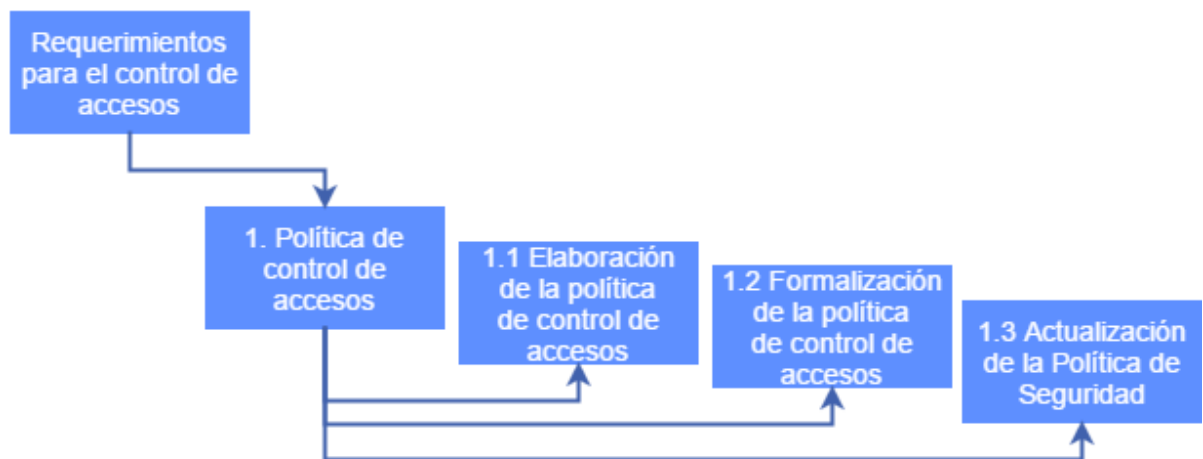


Ilustración 4.6-13

## **Requerimientos para el control de accesos**

### **1. Política de control de accesos**

- 1.1. Elaboración de la política de control de accesos: Se procede a elaborar la política de control de accesos considerando todos los aspectos que sean necesarios incluir en la misma. (ver 4.6.1.1.1(política de control de accesos))
- 1.2. Formalización de la política de control de accesos: la política de control de accesos es evaluada y aprobada por el comité de seguridad de la información. Posteriormente se formaliza la misma (se distribuye el documento a las personas que corresponda).
- 1.3. Actualización de la Política de seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Política de control de accesos) trabajada.

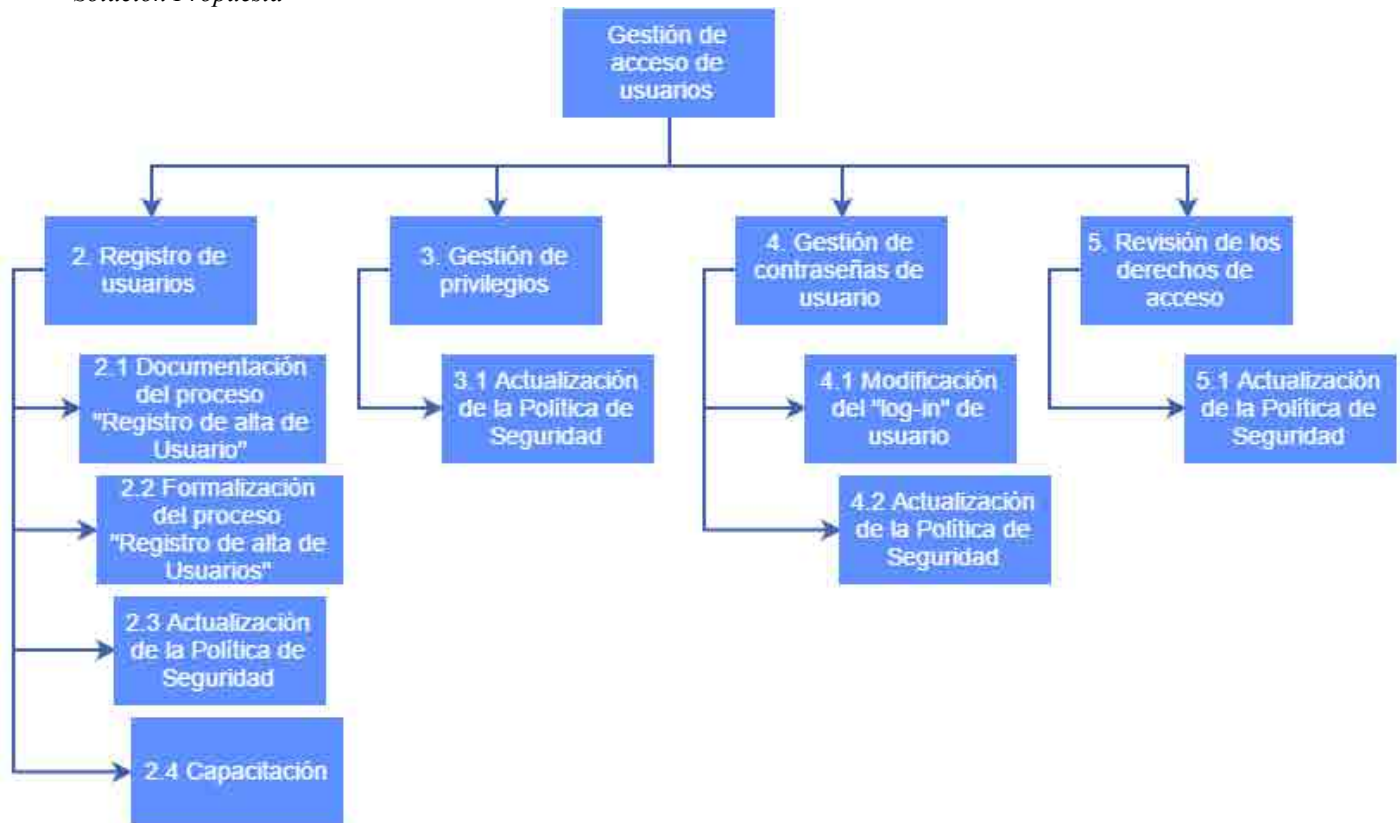


Ilustración 4.6-14

## **Gestión de acceso de usuarios**

### **2. Registro de usuarios.**

- 2.1. Documentación del proceso "Registro de alta de Usuario": Se procede a documentar el proceso teniendo en cuenta todas las modificaciones/mejoras que deben ser consideradas aplicar al mismo.
- 2.2. Formalización del proceso "Registro de alta de Usuarios": el proceso es evaluado y aprobado por el comité de seguridad de la información. Posteriormente se formaliza el mismo (se distribuye el documento a las personas que corresponda).
- 2.3. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Registro de Usuarios) trabajada.
- 2.4. Capacitación: se capacita al personal involucrado en el proceso con el propósito de que las tareas sean realizadas conforme a lo establecido previamente

### **3. Gestión de privilegios.**

- 3.1. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Gestión de privilegios) trabajada.

### **4. Gestión de contraseñas de usuario.**

- 4.1. Modificación del "log-in" de usuario: Se procede a mejorar el proceso de "log-in" del usuario. El mismo es modificado de manera tal que, para la entrega de credenciales (usuario y contraseña), se haga uso de contraseñas temporales (El usuario en su primer ingreso al sistema debe cambiar la contraseña temporal otorgada en primera instancia)

4.2. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Gestión de contraseñas de usuario) trabajada.

5. Revisión de los derechos de acceso.

5.1. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Revisión de los derechos de acceso) trabajada.



Ilustración 4.6-15

**Responsabilidades del usuario**

6. Uso de contraseñas

6.1. Elaboración de la "Guía de buenas prácticas para la selección y uso de contraseñas": Se procede a elaborar un documento en el cual se detallan pautas a seguir para un adecuado uso y selección de contraseñas. Para esta tarea se utiliza como base de elaboración la documentación propuesta en 4.6.3.1.1(Usos de contraseñas)

6.2. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Uso de contraseñas) trabajada.

6.3. Distribución de la guía: Se procede a distribuir la guía en la institución con la finalidad de que la misma sea conocida por toda persona perteneciente a la institución.

7. Equipamiento de usuario que se deja desatendido

7.1. Actualización de la documentación: Se procede a actualizar la documentación correspondiente ("Normativa de uso de los recursos informáticos", "Declaración de los derechos de acceso"), con el propósito de plasmar la importancia del cuidado de los equipos de usuarios que son desatendidos.

6.4. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Equipamiento de usuario que se deja desatendido) trabajada.

8. Política de pantalla y escritorio limpio

5.2. Elaboración y Formalización de la "Política de pantalla de escritorio limpio": Se procede a elaborar la política de resguardo considerando todos los aspectos que sean necesarios incluir en la misma. La política es evaluada y aprobada por el comité de seguridad de la información. Posteriormente se formaliza la misma (se distribuye el documento a las personas que corresponda).

8.1. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Política de pantalla y escritorio limpio) trabajada.

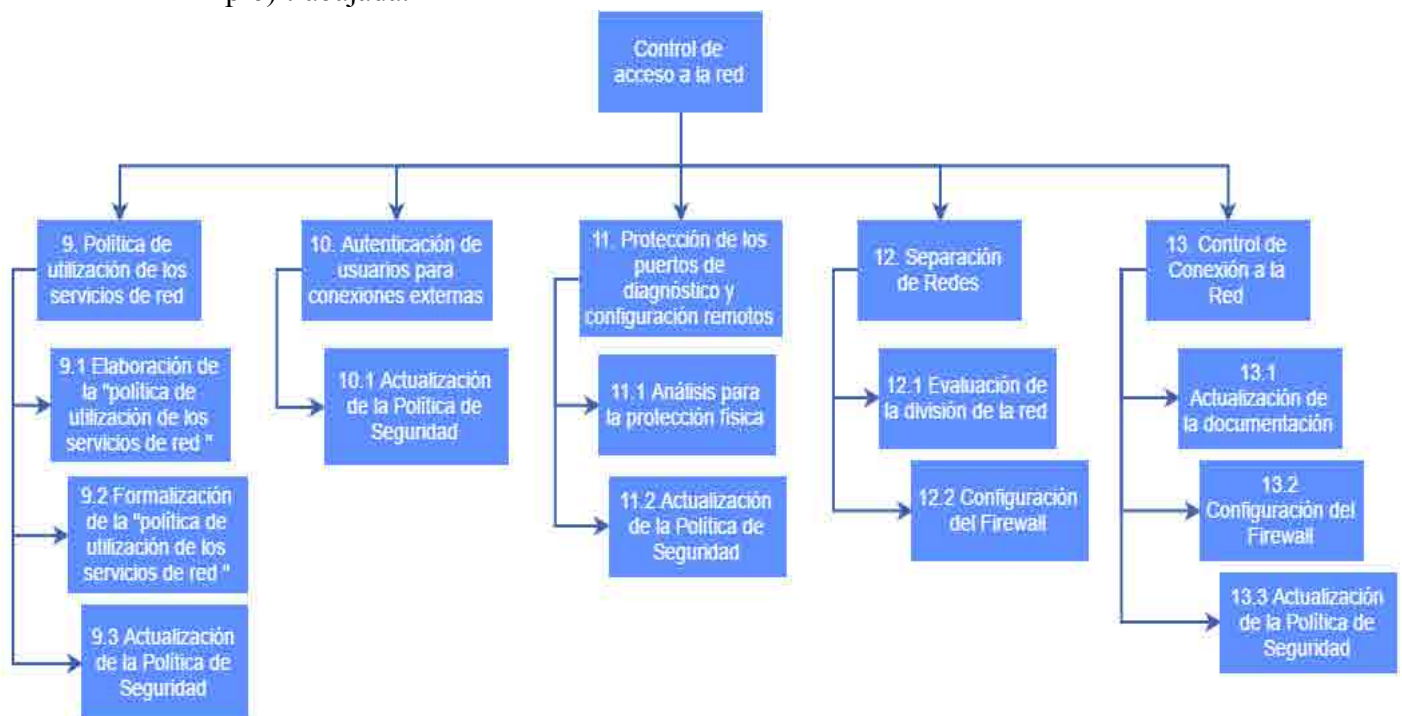


Ilustración 4.6-16

**Control de acceso a la red**

9. Política de utilización de los servicios de red

9.1. Elaboración de la "política de utilización de los servicios de red ": Se procede a elaborar la política de resguardo considerando todos los aspectos que sean necesarios incluir en la misma.

9.2. Formalización de la "política de utilización de los servicios de red ": La política es evaluada y aprobada por el comité de seguridad de la información. Posteriormente se formaliza la misma (se distribuye el documento a las personas que corresponda).

8.2. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Política de Utilización de los servicios de red) trabajada.

10. Autenticación de usuarios para conexiones externas

10.1. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Autenticación de usuarios para conexiones externas) trabajada.

11. Protección de los puertos de diagnóstico y configuración remotos

11.1. Análisis para la protección física: se determina la metodología a utilizar para proteger físicamente a los equipos de red. Una vez determinada la metodología la misma se implemente a todos los equipos de red de la institución.

11.2. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Protección de los puertos de diagnóstico y configuración remotos) trabajada.

12. Separación de Redes

12.1. Evaluación de la división de la red: se realiza un estudio para determinar en cuantas subredes es conveniente dividir la red, analizando los riesgos y posibles complicaciones de realizar esta división.

12.2. Configuración del Firewall: se procede a configurar el Firewall de la institución con el propósito de dividir la red en VLANs según lo establecido previamente.

13. Control de Conexión a la Red

13.1. Actualización de la documentación: Se procede a actualizar la documentación correspondiente (política de control de accesos), de manera tal que la misma incluya entre sus lineamientos lo propuesto en “Control de conexión a la red”

13.2. Configuración del Firewall: el Firewall de la institución es configurado con el propósito que el mismo incluya los filtros adicionales propuestos en “Control de conexión a la red”

13.3. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Control de Conexión a la red) trabajada

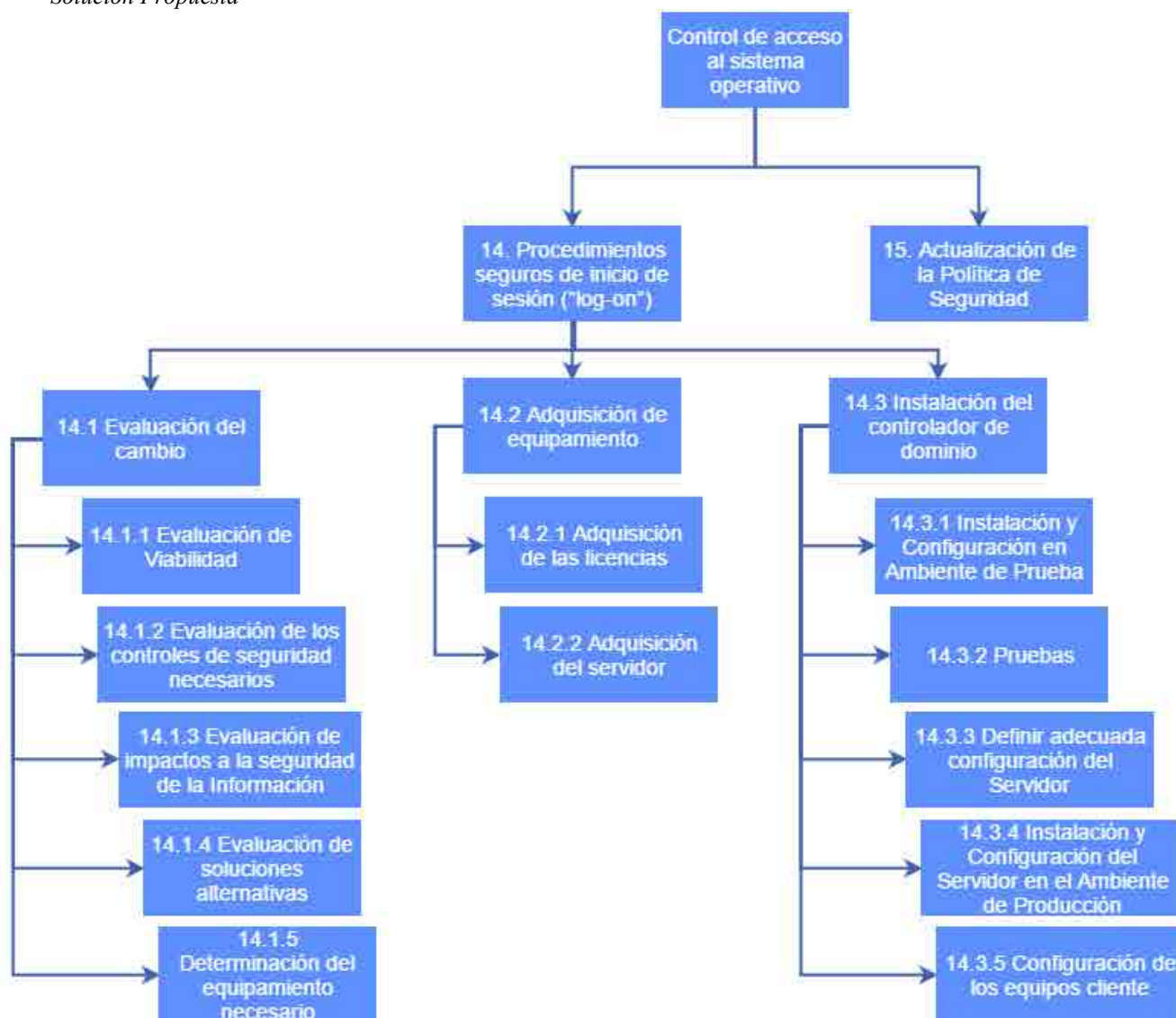


Ilustración 4.6-17

### **Control de acceso al sistema operativo**

#### **14. Procedimientos seguros de inicio de sesión ("log-on")**

##### **14.1. Evaluación del cambio**

- 14.1.1. Evaluación de Viabilidad: Se realiza un análisis con el objeto de determinar si es posible llevar a cabo la solución propuesta
- 14.1.2. Evaluación de los controles de seguridad necesarios: Se realiza un análisis de la importancia de la información involucrada y se determinan los controles de seguridad que deben ser aplicados
- 14.1.3. Evaluación de impactos a la seguridad de la Información: Se realiza un análisis para determinar los posibles impactos que podría causar la implementación de la solución propuesta sobre la integridad de la información manejada.
- 14.1.4. Evaluación de soluciones alternativas: Se evalúan soluciones alternativas a la propuesta

- 14.1.5. Determinación del equipamiento necesario: De acuerdo a la solución seleccionada, se procede a evaluar los requerimientos de equipamiento para implementar apropiadamente la misma.
- 14.2. Adquisición de equipamiento
  - 14.2.1. Adquisición de las licencias: Se procede a adquirir las licencias de software que sean necesarias para la implementación de la solución.
  - 14.2.2. Adquisición del servidor: se procede a adquirir el equipamiento de hardware necesario para la apropiada puesta en marcha del servidor.
- 14.3. Instalación del controlador de dominio
  - 14.3.1. Instalación y Configuración en Ambiente de Prueba: se procede a realizar la instalación del software y configuración en un ambiente de prueba. El software será configurado según las necesidades de la institución y el ambiente de prueba será lo más próximo a la realidad. Además, se seleccionan los equipos (que utilizan el controlador de dominio) con los que se trabajara en las pruebas y se procede a configurar en dichos equipos de manera adecuada (licencia y configuración para comunicarse con el controlador de dominio)
  - 14.3.2. Pruebas: Se realizan pruebas con el objetivo de verificar si se obtiene el resultado deseado en el funcionamiento del software, así como también, se estudia dicho funcionamiento con el propósito de conocer con más profundidad el mismo y para detectar posibles problemas o limitaciones
  - 14.3.3. Definir adecuada configuración del Servidor: Se procede a realizar la configuración en el servidor/equipos de los diferentes aspectos que se deben tener en cuenta según lo establecido en “*Procedimientos seguros de inicio de sesión (“log-on”)*”
  - 14.3.4. Instalación y Configuración del Servidor en el Ambiente de Producción: se procede a realizar la instalación del software en su correspondiente servidor y a llevar al ambiente productivo la configuración previamente testada del software en cuestión
  - 14.3.5. Creación y entrega de usuarios: Se entrega a los usuarios autorizados las credenciales de acceso a los equipos.
  - 14.3.6. Configuración de los equipos cliente: se procede a configurar de manera adecuada los equipos cliente para que estos trabajen apropiadamente con el controlador de dominio y cumplan con todas las configuraciones/controles requeridos.
- 15. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Control de acceso al sistema operativo) trabajada

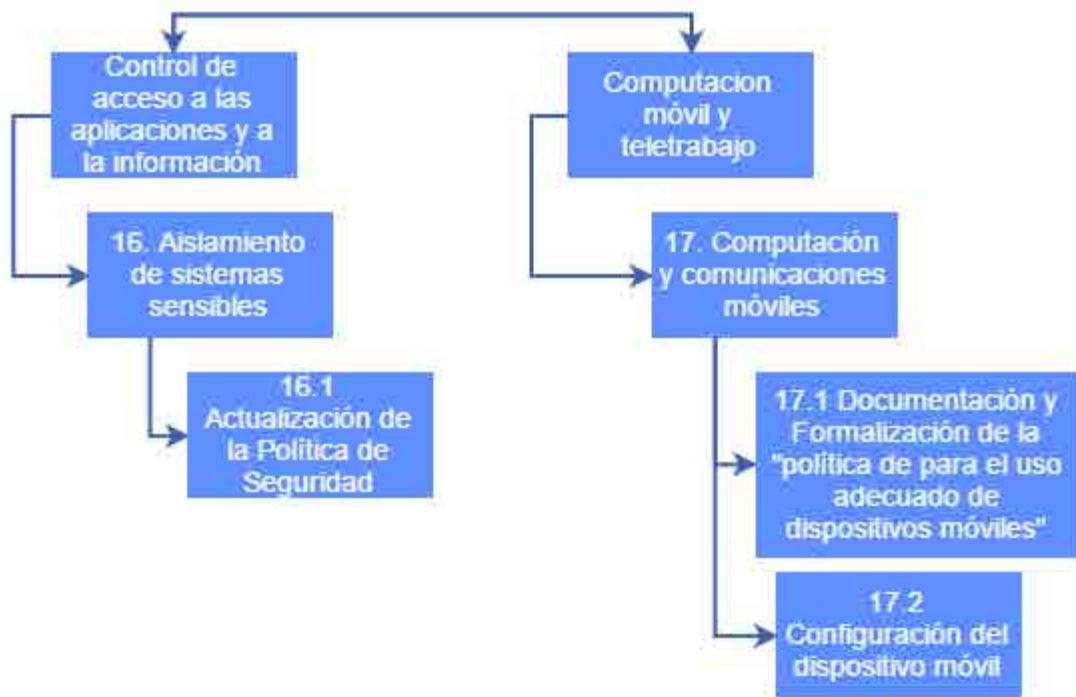


Ilustración 4.6-18

#### **Control de acceso a las aplicaciones y a la información**

##### **16. Aislamiento de sistemas sensibles**

- 16.1. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Aislamiento de sistemas sensibles.) trabajada

#### **Computación móvil y teletrabajo**

##### **17. Computación y comunicaciones móviles**

- 17.1. Documentación y Formalización de la "política de para el uso adecuado de dispositivos móviles": Se procede a elaborar la política considerando todos los aspectos que sean necesarios incluir en la misma. La política es evaluada y aprobada por el comité de seguridad de la información. Posteriormente se formaliza la misma (se distribuye el documento a las personas que corresponda).
- 17.2. Configuración del dispositivo móvil: Se configuran los equipos móviles de la institución conforme a lo establecido en la política previamente mencionada.

##### **4.6.8.3 Estimación de tiempos**

Seguidamente, se establecen los tiempos y recursos para cada una de las actividades previamente detalladas.

UCS - Facultad de Ingeniería  
Revisión de los Procesos de Seguridad del Hospital Dr. Arturo Oñativia  
Solución Propuesta

|    | Nombre                                                                     | Duración | Predecesoras | Recursos                                                                             |
|----|----------------------------------------------------------------------------|----------|--------------|--------------------------------------------------------------------------------------|
| 1  | <input type="checkbox"/> Control de Accesos                                | 104.17d  |              |                                                                                      |
| 2  | Inicio de tareas de Control de Accesos                                     | 0h       |              |                                                                                      |
| 3  | <input type="checkbox"/> Requerimientos para el control de accesos         | 10.33d   |              |                                                                                      |
| 4  | <input type="checkbox"/> Política de control de accesos                    | 10.33d   |              |                                                                                      |
| 5  | Elaboración de la política de control de accesos                           | 20h      | 2            | Responsable de Seguridad de la Información, Jefe del Sector de Sistemas Informáticos |
| 6  | Formalización de la política de control de accesos                         | 6h       | 5            | Comité de Seguridad de la Información                                                |
| 7  | Actualización de la Política de Seguridad                                  | 2h       | 6            | Responsable de Seguridad de la Información                                           |
| 8  | <input type="checkbox"/> Gestión de acceso de usuarios                     | 18d      |              |                                                                                      |
| 9  | <input type="checkbox"/> Registro de usuarios                              | 6.5d     |              |                                                                                      |
| 10 | Documentación del proceso "Registro de alta de Usuarios"                   | 12h      | 5,7          | Responsable de Seguridad de la Información, Jefe del Sector de Sistemas Informáticos |
| 11 | Formalización del proceso "Registro de alta de Usuarios"                   | 3h       | 10           | Comité de Seguridad de la Información                                                |
| 12 | Actualización de la Política de Seguridad                                  | 2h       | 11           | Responsable de Seguridad de la Información                                           |
| 13 | Capacitación                                                               | 2h       | 10,11        | Jefe del Sector de Sistemas Informáticos                                             |
| 14 | <input type="checkbox"/> Gestión de privilegios                            | 0.33d    |              |                                                                                      |
| 15 | Actualización de la Política de Seguridad                                  | 2h       | 12           | Responsable de Seguridad de la Información                                           |
| 16 | <input type="checkbox"/> Gestión de contraseñas de usuario                 | 17.5d    |              |                                                                                      |
| 17 | Modificación del "log-in" de usuario                                       | 60h      | 2            | Persona del Sector de Sist. Inf.                                                     |
| 18 | Actualización de la Política de Seguridad                                  | 2h       | 15           | Responsable de Seguridad de la Información                                           |
| 19 | <input type="checkbox"/> Revisión de los derechos de acceso                | 0.5d     |              |                                                                                      |
| 20 | Actualización de la Política de Seguridad                                  | 3h       | 18           | Responsable de Seguridad de la Información                                           |
| 21 | <input type="checkbox"/> Responsabilidades del usuario                     | 20.5d    |              |                                                                                      |
| 22 | <input type="checkbox"/> Uso de contraseñas                                | 3d       |              |                                                                                      |
| 23 | Elaboración de la "Guía de buenas prácticas para la selección de usuarios" | 12h      | 20           | Responsable de Seguridad de la Información                                           |
| 24 | Actualización de la Política de Seguridad                                  | 2h       | 23           | Responsable de Seguridad de la Información                                           |
| 25 | Distribución de la guía                                                    | 6h       | 17,23        | Persona del Sector de Sist. Inf.                                                     |
| 26 | <input type="checkbox"/> Equipamiento de usuario que se deja desentendido  | 1.33d    |              |                                                                                      |
| 27 | Actualización de la documentación                                          | 6h       | 24           | Responsable de Seguridad de la Información                                           |
| 28 | Actualización de la Política de Seguridad                                  | 2h       | 27           | Responsable de Seguridad de la Información                                           |
| 29 | <input type="checkbox"/> Política de pantalla y escritorio limpio          | 20.5d    |              |                                                                                      |
| 30 | Elaboración y Formalización de la "Política de pantalla de usuario"        | 20h      | 11           | Comité de Seguridad de la Información                                                |
| 31 | Actualización de la Política de Seguridad                                  | 2h       | 28,30        | Responsable de Seguridad de la Información                                           |
| 32 | <input type="checkbox"/> Control de acceso a la red                        | 29.67d   |              |                                                                                      |
| 33 | <input type="checkbox"/> Política de utilización de los servicios de red   | 6.5d     |              |                                                                                      |
| 34 | Elaboración de la "política de utilización de los servicios de red"        | 12h      | 13,31        | Responsable de Seguridad de la Información, Jefe del Sector de Sistemas Informáticos |
| 35 | Formalización de la "política de utilización de los servicios de red"      | 3h       | 34           | Comité de Seguridad de la Información                                                |
| 36 | Actualización de la Política de Seguridad                                  | 2h       | 35           | Responsable de Seguridad de la Información                                           |

Ilustración 4.6-19

*UCS - Facultad de Ingeniería*  
*Revisión de los Procesos de Seguridad del Hospital Dr. Arturo Oñativia*  
*Solución Propuesta*

|    |                                                           |        |          |                                                                                     |
|----|-----------------------------------------------------------|--------|----------|-------------------------------------------------------------------------------------|
| 37 | ☐Autenticación de usuarios para conexiones externas       | 0.33d  |          |                                                                                     |
| 38 | Actualización de la Política de Seguridad                 | 2h     | 36       | Responsable de Seguridad de la Información                                          |
| 39 | ☐Protección de los puertos de diagnóstico y configuración | 10.5d  |          |                                                                                     |
| 40 | Análisis para la protección física                        | 60h    | 38       | Responsable de Seguridad de la Información                                          |
| 41 | Actualización de la Política de Seguridad                 | 3h     | 40       | Responsable de Seguridad de la Información                                          |
| 42 | ☐Separación de Redes                                      | 7d     |          |                                                                                     |
| 43 | Evaluación de la división de la red                       | 12h    | 41       | Responsable de Seguridad de la Información                                          |
| 44 | Configuración del Firewall                                | 30h    | 34,43    | Responsable de Seguridad de la Información,Jefe del Sector de Sistemas Informáticos |
| 45 | ☐Control de Conexión a la Red                             | 23.5d  |          |                                                                                     |
| 46 | Actualización de la documentación                         | 3h     | 35       | Comité de Seguridad de la Información                                               |
| 47 | Configuración del Firewall                                | 30h    | 44,46    | Responsable de Seguridad de la Información                                          |
| 48 | Actualización de la Política de Seguridad                 | 2h     | 47       | Responsable de Seguridad de la Información                                          |
| 49 | ☐Control de acceso al sistema operativo                   | 42.33d |          |                                                                                     |
| 50 | ☐Procedimientos seguros de inicio de sesión ("log-on")    | 42.33d |          |                                                                                     |
| 51 | ☐Evaluación del cambio                                    | 15.33d |          |                                                                                     |
| 52 | Evaluación de Viabilidad                                  | 20h    | 44       | Jefe del Sector de Sistemas Informáticos                                            |
| 53 | Evaluación de los controles de seguridad necesarios       | 12h    | 48       | Responsable de Seguridad de la Información                                          |
| 54 | Evaluación de impactos a la seguridad de la Informa       | 12h    | 53       | Responsable de Seguridad de la Información                                          |
| 55 | Evaluación de soluciones alternativas                     | 30h    | 52,54    | Responsable de Seguridad de la Información,Jefe del Sector de Sistemas Informáticos |
| 56 | Determinación del equipamiento necesario                  | 6h     | 55       | Responsable de Seguridad de la Información,Jefe del Sector de Sistemas Informáticos |
| 57 | ☐Adquisición de equipamiento                              | 20d    |          |                                                                                     |
| 58 | Adquisición de las licencias                              | 60h    | 56       | Personal del Sector de Compras                                                      |
| 59 | Adquisición del servidor                                  | 60h    | 58       | Personal del Sector de Compras                                                      |
| 60 | ☐Instalación del controlador de dominio                   | 27d    |          |                                                                                     |
| 61 | Instalación y Configuración en Ambiente de Prueba         | 30h    | 56       | Responsable de Seguridad de la Información,Jefe del Sector de Sistemas Informáticos |
| 62 | Pruebas                                                   | 30h    | 61       | Responsable de Seguridad de la Información,Jefe del Sector de Sistemas Informáticos |
| 63 | Definir adecuada configuración del Servidor               | 18h    | 62       | Responsable de Seguridad de la Información                                          |
| 64 | Instalación y Configuración del Servidor en el Ambie      | 12h    | 59,62,63 | Responsable de Seguridad de la Información,Jefe del Sector de Sistemas Informáticos |
| 65 | Creación y entrega de usuarios                            | 18h    | 64       | Responsable de Seguridad de la Información                                          |
| 66 | Configuración de los equipos cliente                      | 30h    | 25,64    | Persona del Sector de Sist. Inf.                                                    |
| 67 | Actualización de la Política de Seguridad                 | 4h     | 65       | Responsable de Seguridad de la Información                                          |
| 68 | ☐Control de acceso a las aplicaciones y a la información  | 0.5d   |          |                                                                                     |
| 69 | ☐Aislamiento de sistemas sensibles                        | 0.5d   |          |                                                                                     |
| 70 | Actualización de la Política de Seguridad                 | 3h     | 67       | Responsable de Seguridad de la Información                                          |
| 71 | ☐Computación móvil y teletrabajo                          | 54.83d |          |                                                                                     |
| 72 | ☐Computación y comunicaciones móviles                     | 54.83d |          |                                                                                     |
| 73 | Documentación y Formalización de la "política de para e   | 20h    | 46       | Comité de Seguridad de la Información                                               |
| 74 | Configuración del dispositivo móvil                       | 3h     | 66,73    | Persona del Sector de Sist. Inf.                                                    |
| 75 | Fin de tareas de Control de Accesos                       | 0h     | 70,74    |                                                                                     |

*Ilustración 4.6-20*

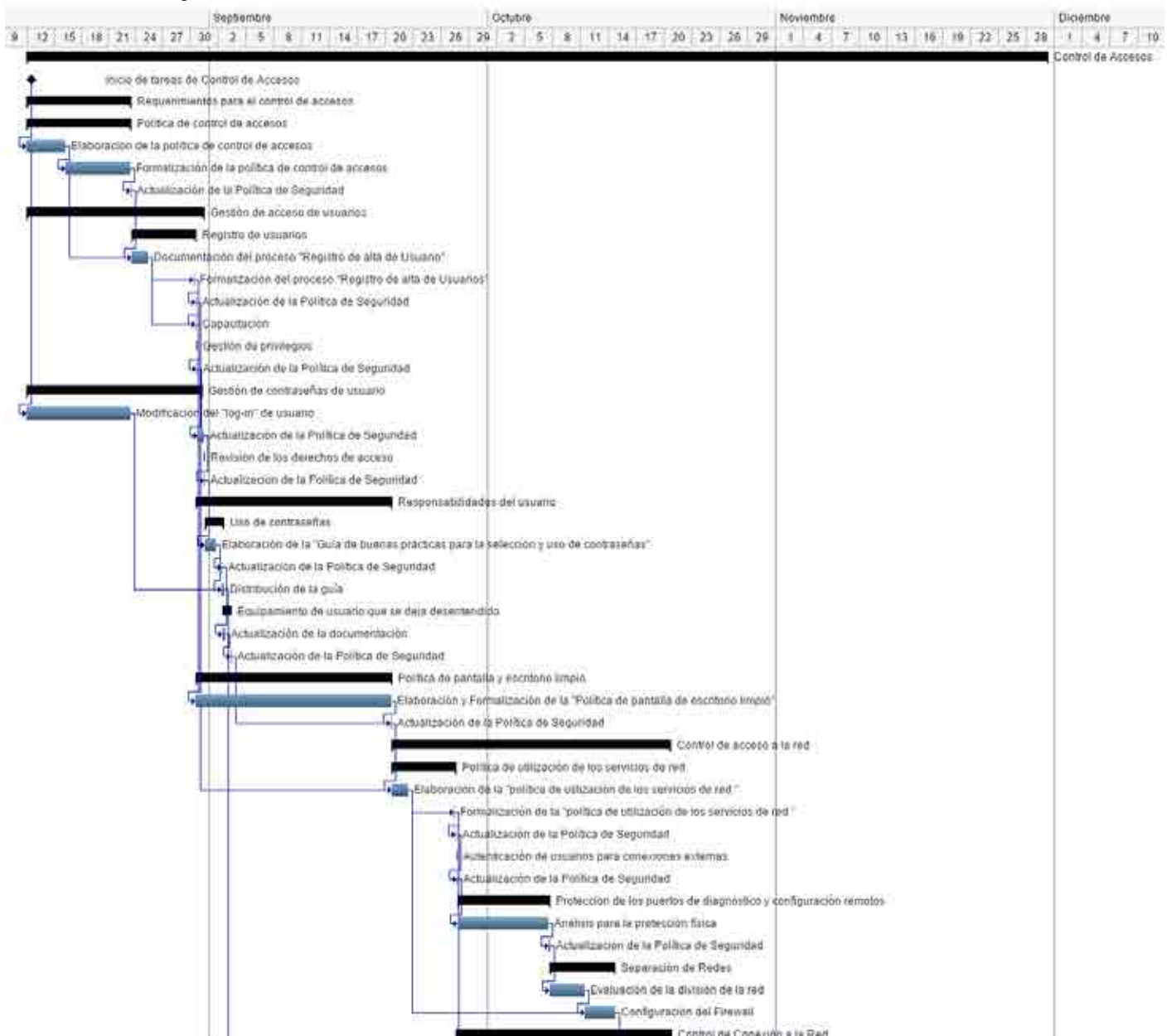


Ilustración 4.6-21

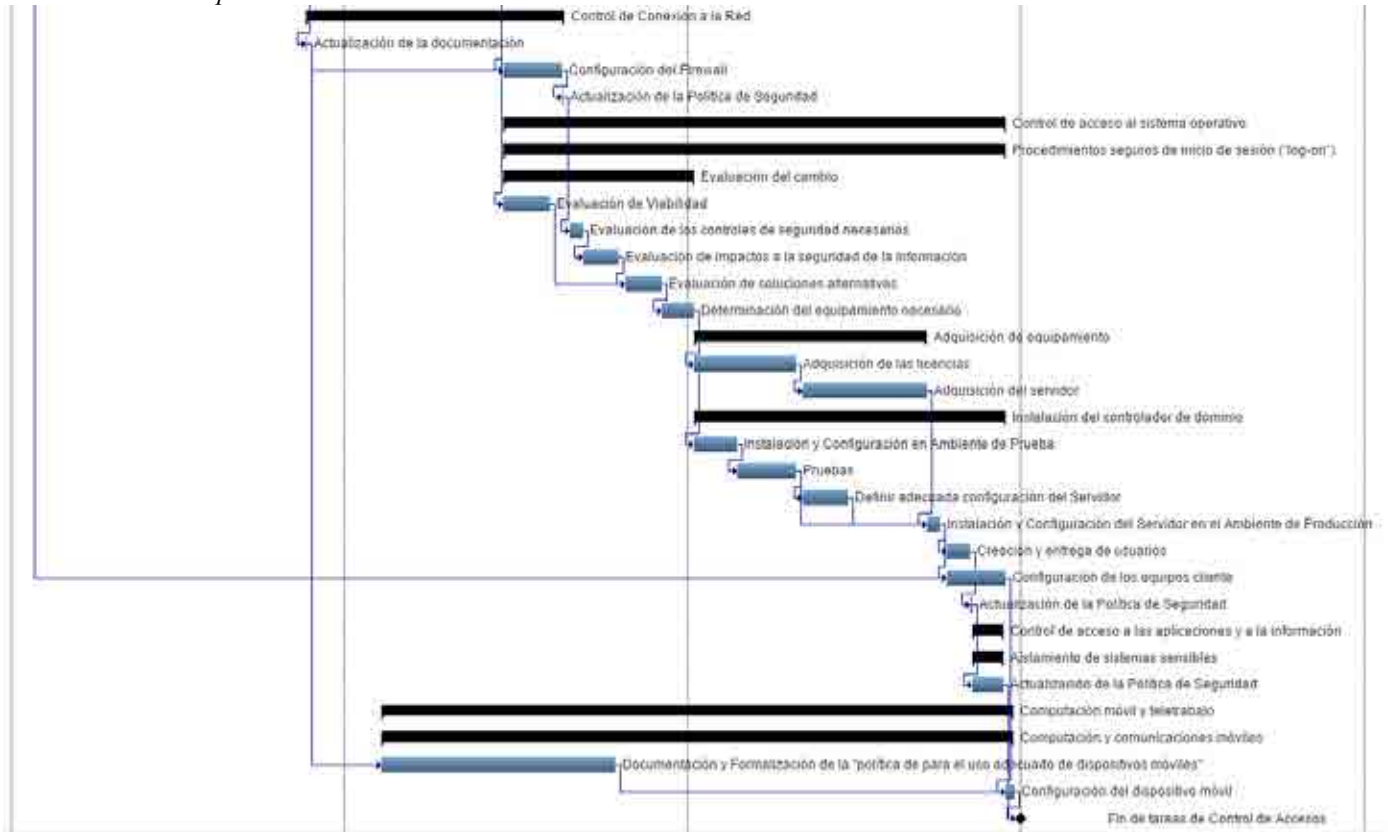


Ilustración 4.6-22

#### 4.6.9 Análisis de Riesgos

Se establecen los riesgos a los que está expuesta la institución al no realizar una adecuada gestión de Control de Accesos.

| Riesgo                                                                                                            | Impacto   | Probabilidad | Importancia | Prevención                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------|-----------|--------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Fuga de Información, debido al uso malicioso de recursos tecnológicos por parte de personas no autorizadas</b> | <b>10</b> | <b>0,3</b>   | <b>3</b>    | <b>Adecuado uso de contraseñas de usuario</b><br><br><b>Concientización sobre el cuidado de equipos desatendidos</b><br><br><b>Políticas de pantallas y escritorio limpio</b><br><br><b>Autenticación de conexiones externas y protección de puertos</b><br><br><b>Adecuado control de acceso a los sistemas operativos (Controlador de dominio)</b> |

|                                                                                                         |            |             |            |                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------|------------|-------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                         |            |             |            | <u>Políticas apropiadas para el cuidado y uso de dispositivos móviles (protección de la información contenida en los mismos)</u>                                                      |
| <u>Saturación de la red disponible en la institución (afecta a la disponibilidad de la información)</u> | <u>4</u>   | <u>0,75</u> | <u>3</u>   | <u>Adecuados controles de acceso a la red</u><br><u>Políticas de uso de la red</u><br><u>Separación de redes</u>                                                                      |
| <u>Uso indebido de recursos tecnológicos por parte del personal autorizado</u>                          | <u>0,8</u> | <u>2</u>    | <u>1,6</u> | <u>Controlador de Dominio (Control de acceso al sistema operativo)</u><br><u>Restricción de acceso a las aplicaciones</u>                                                             |
| <u>Pérdida de información debido a acceso no autorizados en la red</u>                                  | <u>0,2</u> | <u>3</u>    | <u>0,6</u> | <u>Adecuado uso de contraseñas de usuario</u><br><u>Adecuada gestión de contraseñas de equipamiento de red</u><br><u>Autenticación de conexiones externas y protección de puertos</u> |

Tabla 4.6-25

#### 4.6.10 Análisis Económico-Financiero

##### 4.6.10.1 Estimación de costos

A continuación, se detallan los costos necesarios para implementar las mejoras propuestas

- **Hardware:** En cuanto a costos de Hardware, se registra la adquisición de 1 servidor para la instalación del “Controlador de Dominio” mencionado en 4.6.5.1.1(Procedimientos seguros de inicio de sesión (“log-on”)).

| HARDWARE     |                  |                 |           |
|--------------|------------------|-----------------|-----------|
| ITEM         | CANTIDAD         | PRECIO UNITARIO | TOTAL     |
| Servidor     | 1                | \$ 30.000       | \$ 30.000 |
| <b>Total</b> | <b>\$ 30.000</b> |                 |           |

Tabla 4.6-26

- Software: Se registra la adquisición de las licencias para el servidor Windows, y las correspondientes licencias de conexión 4.6.5.1.1(Procedimientos seguros de inicio de sesión (“log-on”)).

| SOFTWARE                                                  |                     |                            |              |
|-----------------------------------------------------------|---------------------|----------------------------|--------------|
| ITEM                                                      | CANTIDAD            | PRECIO UNITARIO            | TOTAL        |
| Licencia de Windows Server 2012                           | 1                   | \$ 8.000                   | \$ 8.000     |
| Licencias de Conexión al Servidor (5 licencias de acceso) | 28                  | \$ 2.872,80 <sup>156</sup> | \$ 80.438,40 |
| <b>Total</b>                                              | <b>\$ 88.438,40</b> |                            |              |

Tabla 4.6-27

- Recursos Humanos: Debido a que el personal de Sistemas Informáticos en colaboración con el responsable de seguridad de la información son los encargados de llevar adelante la instalación y configuración correspondiente, así como también la elaboración del registro de activos de información, no se registran costos en este concepto.

#### 4.6.10.2 Beneficios Operativos

Llevar a cabo las recomendaciones realizadas en los controles previamente analizados, proveerán a la institución de los siguientes beneficios:

- Facilidad en la gestión de derechos de accesos (red y sistemas operativos).
- Rápida obtención de información relacionada al usuario y a las estaciones de trabajo (Auditoria).

<sup>156</sup> Valores publicados por la tienda oficial de Microsoft al día de la fecha (30/08/2016) (u\$d 189,00). Se transforma a pesos argentinos aplicando la cotización del día (\$ 15,28).

Yustman, Mauricio Ezequiel

- Centralización de la información de cuentas de usuario. Esto facilita la protección de los datos de usuario (derechos de acceso, contraseñas) de accesos no autorizados. También, permite realizar con mayor facilidad los resguardos de estos datos.
- Reducción de accesos no autorizados a los recursos informáticos/información.
- Mayor control sobre las estaciones de trabajo del usuario.
- Promoción de la seguridad de la información en la institución. (protección de las estaciones de trabajo, uso de contraseñas robustas).

#### 4.6.10.3 Análisis Económico

En base a los riesgos definidos, identificamos y estimamos el valor de cada uno de los activos que pueden verse afectados por los mismos, para lo cual, consideramos el tiempo y los recursos que son necesarios invertir para recuperar o recrear el activo en cuestión:

| Amenazas                                                                                                   | Activos               | Tiempo Estimado de Recuperación                                                                                         | Recursos         | Tiempo Total | Salario por Hora <sup>157</sup> | Valor del Activo            |
|------------------------------------------------------------------------------------------------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------|------------------|--------------|---------------------------------|-----------------------------|
| Fuga de Información, debido al uso malicioso de recursos tecnológicos por parte de personas no autorizadas | Activo de Información | **En caso de Fuga de Información, pueden existir costos legales, y puede ser necesario indemnizar a la persona afectada | -                | -            | -                               | \$605.897,52 <sup>158</sup> |
| Uso indebido de recursos tecnológicos por parte del personal autorizado                                    | Activo de Información | 8 horas <sup>159</sup>                                                                                                  | 1 persona (Inf.) | 8 horas      | \$133,00                        | \$1.064,00                  |
|                                                                                                            | Activo de Software    | 4 horas <sup>160</sup>                                                                                                  | 1 persona (Inf.) | 4 horas      | \$133,00                        | \$532,00                    |
| Pérdida de información debido a acceso                                                                     | Activo de Información | 3 horas <sup>161</sup>                                                                                                  | 140 personas     | 420 horas    | \$133,00                        | \$55.860,00                 |

<sup>157</sup> Se utilizó un Salario mensual de \$16000 con 30 hs semanales de trabajo.

<sup>158</sup> Se estima a partir de la fórmula de Vuotto, con  $n=23,5$  y  $a=48750$  (salario mensual de \$15.000 y un porcentaje de incapacidad de 0,25). Daño por la información filtrada.

<sup>159</sup> Tiempo aproximado en recuperar un gran número de registros eliminados o modificados por un usuario con acceso mal concedido.

<sup>160</sup> Tiempo aproximado para formatear una PC, debido a que el usuario disponía de permisos administrativos en el sistema operativo.

<sup>161</sup> Se estima la pérdida de información de 1 día laboral. Se toma un promedio de 3 horas para que cada empleado cargue nuevamente la información generada en el día.

|                                                                                                  |                       |                       |              |           |          |             |
|--------------------------------------------------------------------------------------------------|-----------------------|-----------------------|--------------|-----------|----------|-------------|
| no autorizados en la red                                                                         |                       |                       |              |           |          |             |
| Saturación de la red disponible en la institución (afecta a la disponibilidad de la información) | Activo de Información | 1 hora <sup>162</sup> | 140 personas | 140 horas | \$133,00 | \$18.620,00 |

Tabla 4.6-28

A continuación, calculamos la Expectativa de Pérdida Individual para cada uno de los activos identificados anteriormente:

| Activo                | Amenaza                                                                                                    | Valor del Activo | EF (Factor de Exposición) | SLE (Expectativa de Pérdida Individual) |
|-----------------------|------------------------------------------------------------------------------------------------------------|------------------|---------------------------|-----------------------------------------|
| Activo de Información | Fuga de Información, debido al uso malicioso de recursos tecnológicos por parte de personas no autorizadas | \$605.897,52     | 0,65                      | \$393.833,39                            |
| Activo de Información | Uso indebido de recursos tecnológicos por parte del personal autorizado                                    | \$1.064,00       | 0,5                       | \$532,00                                |
| Activo de Software    |                                                                                                            | \$532,00         | 0,5                       | \$266,00                                |
| Activo de Información | Pérdida de información debido a acceso no autorizados en la red                                            | \$55.860,00      | 0,6                       | \$33.516,00                             |
| Activo de Información | Saturación de la red disponible en la institución (afecta a la disponibilidad de la información)           | \$18.620,00      | 0,5                       | \$9.310,00                              |

Tabla 4.6-29

Con el propósito de calcular la Expectativa de Pérdida Anual (ALE), se realizó una estimación de la Tasa de Ocurrencia Anualizada (ARO), debido a la inexistencia de datos históricos de incidentes de seguridad de la información dentro de la organización, y se obtuvieron los siguientes valores:

<sup>162</sup> Se estima que, debido a la congestión de la red, el personal pierde 1 hora de su día laboral.

| Activo                | Amenaza                                                                                                    | SLE (Expectativa de Pérdida Individual) | ARO (Tasa de Ocurrencia Anualizada) | ALE (Expectativa de Pérdida Anual) |
|-----------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------|-------------------------------------|------------------------------------|
| Activo de Información | Fuga de Información, debido al uso malicioso de recursos tecnológicos por parte de personas no autorizadas | \$393.833,39                            | 0,3                                 | \$118.150,02                       |
| Activo de Información | Uso indebido de recursos tecnológicos por parte del personal autorizado                                    | \$532,00                                | 0,8                                 | \$425,60                           |
| Activo de Software    |                                                                                                            | \$266,00                                | 0,8                                 | \$212,80                           |
| Activo de Información | Pérdida de información debido a acceso no autorizados en la red                                            | \$33.516,00                             | 0,2                                 | \$6.703,20                         |
| Activo de Información | Saturación de la red disponible en la institución (afecta a la disponibilidad de la información)           | \$9.310,00                              | 0,75                                | \$6.982,50                         |
| <b>Total</b>          |                                                                                                            |                                         |                                     | <b>\$132.474,12</b>                |

Tabla 4.6-30

Como podemos ver, el total obtenido en la tabla anterior constituye la pérdida anual de la organización por no llevar adelante una adecuada gestión de accesos.

#### 4.7 Adquisición, desarrollo y mantenimiento de sistemas de información

##### 4.7.1 Requerimiento de seguridad de los sistemas de información.

*“Objetivo: Garantizar que la seguridad sea una parte integral de los sistemas de información.”*

*Los sistemas de información incluyen sistemas operativos, infraestructura, aplicaciones de negocio, productos enlatados, servicios y aplicaciones desarrolladas por el usuario. El diseño e implementación del sistema de información que da soporte a los procesos de negocio puede ser crucial para la seguridad. Se recomienda que los requerimientos de seguridad se identifiquen y acuerden antes del desarrollo e implementación de los sistemas de información.*

*Es conveniente que se identifiquen todos los requerimientos de seguridad en la fase de requerimientos de un proyecto y se justifiquen, acuerden y documenten como parte de la actividad del sistema de información.”<sup>163</sup>*

<sup>163</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

### **Control**

*“Se recomienda que las declaraciones de requerimientos de la actividad para nuevos sistemas de información, o mejoras de los sistemas de información existentes, especifiquen las necesidades de controles de seguridad”<sup>164</sup>*

### **Relevamiento**

Con el fin de corroborar el cumplimiento del presente control en el hospital se realizó una entrevista con el jefe del sector de sistemas informáticos, ya que, es responsabilidad del sector la administración y el mantenimiento de los sistemas informáticos.

Durante la entrevista se realizaron las siguientes preguntas, en base a lo establecido en el control *“Análisis y especificaciones de los requerimientos de seguridad”* de la norma IRAM-ISO/IEC 27002:2008:

- Los requerimientos para nuevos sistemas o mejoras en los sistemas de información, ¿Incorporan necesidades de controles de seguridad?
- ¿Se consideran controles automáticos y controles manuales de seguridad?
- ¿Los controles de seguridad reflejan el valor para la institución de los activos de información involucrados?
- ¿Estos controles se integran en etapas tempranas del desarrollo?
- En caso de adquirir software de un tercero, en el contrato ¿se incluyen los requerimientos de seguridad necesarios que debe cumplir el software? Si el producto no cumple con lo especificado, ¿Qué medidas se consideran?

Es importante destacar que no existe en la institución un proceso formal a través del cual se obtenga un registro de los requerimientos para mejoras al sistema existente, por lo cual no fue posible el análisis de este documento para realizar el estudio del presente control.

En base a la información obtenida durante la entrevista, se determinó que, cuando son requeridos cambios/mejoras en los sistemas, los requerimientos que deben cumplir no incluyen controles de seguridad. Los controles de seguridad que se aplican actualmente son básicos, como por ejemplo la administración de permisos (lectura, escritura, modificación, eliminación), autenticación de usuario, roles de sistema (administrador, usuario común), limitación de acceso (un usuario solo puede visualizar y acceder a los módulos para los que fue autorizado) y son aplicados a toda mejora/cambio que se realice según sea necesario. Los controles de seguridad antes mencionado son incluidos en etapas tempranas de desarrollo, pero también son implementados en las etapas finales (por ejemplo, cuando se incorporan usuarios que necesiten hacer uso de esta mejora/cambio). Es por esto, que consideramos que el presente control no se cumple dentro de la institución.

En cuanto al software adquirido a terceros, no fue posible un correcto análisis del presente control debido a que, los contratos/acuerdos celebrados con terceros son manejados por el Ministerio de Salud de la provincia de Salta y este el encargado de tomar las decisiones

---

<sup>164</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

que se consideren necesarias sobre las características/requerimientos que debe cumplir el software.

#### 4.7.1.1.1 Cambios recomendados

Con el propósito de formalizar un proceso mediante el cual se obtenga un documento en el cual se detallen los requerimientos de un cambio/mejora al sistema de información existente, recomendamos adoptar la solución propuesta en **4.5.1.2.1** (gestión de cambios). Esto brindará al sector de informática un proceso formal a través del cual se pueden controlar los cambios/mejoras al sistema de manera adecuada.

Con el objetivo de cumplimentar lo propuesto por el presente control, recomendamos ampliar las tareas realizadas en “*Evaluación de cambio*” del proceso mencionado en **4.5.1.2** (gestión de cambios). En la etapa antes mencionada del proceso, debe evaluarse, además, los controles de seguridad que serán necesarios aplicar al cambio en cuestión. Es importante contar en esta etapa con la colaboración del responsable de seguridad de la información. Para determinar los controles de seguridad necesarios, debe considerarse el valor/importancia de los datos involucrados, es por ello que, en primer lugar, debe evaluarse la importancia que tienen los datos para la institución. (ver **4.3** “gestión de activos”). Esto ayudará a definir controles de seguridad acordes al valor de la información.

Los controles de seguridad necesarios para el cambio/mejora a implementar, deben ser plasmados en un documento en donde se detallen los mismos. Esto ayudará a disponer de dos documentos de gran importancia para el diseño y desarrollo del cambio/mejora: Un documento con los requerimientos del cambio/mejora y otro con los controles de seguridad que deben aplicarse.

Algunos controles de seguridad adicionales a los existentes que pueden ser considerados son:

- Control de Transacciones: puede solicitarse cierta autenticación (clave) para que determinada transacción sea procesada por el sistema.
- Limitaciones de Horario: ciertas funcionalidades del sistema podrían estar disponible en un determinado horario.
- Limitaciones de Ubicación: ciertas funcionalidades del sistema podrían estar disponibles en un determinado sector o en una determinada estación de trabajo.

#### 4.7.2 Procesamiento correcto en las aplicaciones

*“Objetivo: Prevenir errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones.*

*Es conveniente que se diseñen los controles apropiados en las aplicaciones, incluyendo las aplicaciones desarrolladas por los usuarios para asegurar el procesamiento correcto. Se recomienda que estos controles incluyan la validación de los datos de entrada, procesamiento interno y datos de salida.*

*Se puede requerir controles adicionales para los sistemas que procesan o tienen un impacto sobre la información sensible, valiosa o crítica. Es conveniente que se determinen tales controles sobre la base de los requerimientos de seguridad y la evaluación de los riesgos.”<sup>165</sup>*

---

<sup>165</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

### **Control**

*“Se recomienda que los datos de entrada de las aplicaciones se validen para asegurar que son correctos y apropiados”<sup>166</sup>*

### **Relevamiento**

Con el propósito de examinar el cumplimiento del presente control, se realizó una entrevista al Jefe del Sector de Sistemas Informáticos, dado que, es responsabilidad del sector la administración y el mantenimiento de los sistemas informáticos

De acuerdo a lo establecido en el control “Validación de los datos de entrada” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:

- ¿Son validados los datos de entradas de las aplicaciones mediante controles específicos?  
¿Qué tipo de controles se aplican?
- ¿Qué medidas extras se consideran para controlar los datos de entrada?

Conforme a los datos obtenidos durante la entrevista realizada el día 09/06/2016, se completó el siguiente Checklist:

| Validación de los datos de entrada                                                            | Sí | No |
|-----------------------------------------------------------------------------------------------|----|----|
| ¿Existen controles para validar los datos de entrada de las aplicaciones?                     | X  |    |
| Se considera controles de entrada tales como:                                                 |    |    |
| Verificar rango de los datos (valor fuera de rango)                                           | X  |    |
| Verificar caracteres (caracteres inválidos en campos de datos)                                | X  |    |
| Verificar que los datos son completos (datos faltantes o incompletos)                         | X  |    |
| Se realizan revisiones periódicas de los datos para confirmar su validez                      |    | X  |
| Se revisan los documentos de entrada para detectar cambios no autorizados                     | X  |    |
| Responsabilidades definidas de todo el personal involucrado en el proceso de entrada de datos |    | X  |
| Existen registro de todas las actividades involucradas en la carga de datos.                  | X  |    |

Tabla 4.7-1

Como puede observarse en el anterior checklist, existen controles para validar los datos de entrada al sistema ERP de la institución. Es importante aclarar que los controles que se aplican varían según el tipo de dato al que se hace referencia y según el módulo/funcionalidad involucrada. Por ejemplo, para ingresar pacientes, existe un control que no permite ingresar al paciente si los datos del mismo (DNI, nombre, apellido, teléfono, etc.) no están completos, a pesar de esto, el sistema permite ingresar pacientes que deben ser atendidos por urgencia y de

<sup>166</sup> IRAM-ISO/IEC 27002:2008  
Yustman, Mauricio Ezequiel

los cuales no se conocen los datos (todos los campos se dejan vacíos) esto permite crear el perfil del paciente en el sistema y cuando sea posible completar los datos faltantes. Por otro lado, otros módulos/funcionalidades del sistema poseen controles típicos del formato de los datos a ingresar (rango, caracteres aceptados, etc.). Toda carga de datos en el sistema es registrada por el mismo sistema, el registro almacena el tipo de dato involucrado, el campo modificado, el valor modificado (nuevo y antiguo valor) y el usuario que realizó el evento. Por último, cuando surgen problemas, los documentos en papel son revisados para detectar cambios no autorizados y así determinar el responsable de este cambio. Debido a esto consideramos que el presente control se cumple parcialmente en la institución.

Es necesario aclarar que, las revisiones sobre la carga de los datos, actualmente se realizan ante la existencia de algún problema y que no existen responsabilidades definidas para la carga de los datos. Es por esto que ciertos puntos del presente control no se cumplen en la institución.

#### 4.7.2.1.1 Cambios recomendados

Con el objetivo de cumplimentar con todos los puntos propuestos por el presente control, recomendamos que, además de utilizar la validación automática que actualmente posee el sistema ERP de la institución, se consideren llevar a cabo los siguientes controles:

- Realizar revisiones periódicas para confirmar la validez de los datos ingresados en el sistema. Esta tarea debe ser realizada por el jefe/responsable de cada sector. Para realizar estas revisiones debe considerarse el volumen de datos manejado por cada sector y debe definirse un adecuado procedimiento para realizar las mismas, debido a que, si se posee un gran volumen de datos será imposible para una sola persona revisar todos los datos ingresados (se podría evaluar una determinada cantidad de registros como muestra del total de los datos)
- Es necesario definir claramente las responsabilidades del personal involucrado en la carga de datos. Se debe entregar a aquellas personas encargadas de la carga de datos un documento en el cual se detallen las responsabilidades que tienen en la carga de datos. Esto ayudará a garantizar que la entrada de los datos tenga como primer control a la misma persona encargada de esto. El documento debe ser elaborado por el comité de seguridad de la información y aprobado por la gerencia.

#### 4.7.2.2 Controles de procesamiento interno

##### **Control**

*“Se recomienda que las verificaciones de validación se incorporen a las aplicaciones para detectar cualquier caso de corrupción de la información, a través de errores de procesamiento o actos deliberados”<sup>167</sup>*

##### **Relevamiento**

Para verificar el cumplimiento del presente control dentro de la organización se procedió a realizar una entrevista al Jefe del Sector de Sistemas Informáticos, ya que, es responsabilidad del sector la administración y el mantenimiento de los sistemas informáticos

---

<sup>167</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

Teniendo en cuenta lo establecido en el control “*Controles de procesamiento interno*” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:

- ¿Se implementan controles de validación con el objetivo de detectar una posible corrupción de la información a causa del mal procesamiento de la misma o por un acto deliberado?

Conforme a los datos obtenidos durante la entrevista realizada al jefe del sector de sistemas informáticos, realizada el día 09/06/2016, se completó el siguiente Checklist:

| Controles de procesamiento interno                                                               | Sí | No |
|--------------------------------------------------------------------------------------------------|----|----|
| Los controles consideran:                                                                        |    |    |
| El uso de funciones de agregado, modificación y de borrado para implementar cambios en los datos |    | X  |
| Los procedimientos para prevenir la ejecución de programas en un orden equivocado                |    | X  |
| El uso de programas apropiados para recuperarse de fallas                                        |    | X  |

Tabla 4.7-2

Cómo es posible apreciar en el checklist, actualmente no se considera ningún tipo de control (más allá de los controles previos al procesamiento como lo es la validación de los datos de entrada) de manera tal de asegurar la integridad de los datos y minimizar los riesgos causados por fallas de procesamiento de los datos o actos deliberados. Es por esto que consideramos que no se cumplimenta con el presente control en la institución.

#### 4.7.2.2.1 Cambios recomendados

Con el objetivo de prevenir errores corrupción de la información, causados por errores de procesamiento o actos deliberados, recomendamos se considere hacer uso de las siguientes herramientas:

- The 2010 CWE/SANS Top 25 Most Dangerous Programming Error ([http://cwe.mitre.org/top25/archive/2010/2010\\_cwe\\_sans\\_top25.pdf](http://cwe.mitre.org/top25/archive/2010/2010_cwe_sans_top25.pdf) Página vigente al 21/06/2016): es un documento que posee una lista de errores de programación que pueden generar vulnerabilidades de software serias.
- GRADUIT: es un script que permite encontrar fallos de seguridad. (para más información <http://www.justanotherhacker.com/projects/graduit.html> Página vigente al 21/06/2016)

Recomendamos el uso de las herramientas previamente mencionadas o similares.

#### 4.7.2.3 Integridad del mensaje

##### **Control**

*“Se recomienda que se identifiquen los requerimientos para asegurar la autenticidad y para proteger la integridad del mensaje en las aplicaciones, así como que se identifiquen e implementen controles apropiados ”<sup>168</sup>*

### **Relevamiento**

Con el fin de corroborar el cumplimiento del presente control en el hospital se realizó una entrevista con el jefe del sector de sistemas informáticos, ya que, es responsabilidad del sector la administración y el mantenimiento de los sistemas informáticos.

Se plantearon los siguientes interrogantes a realizar durante la entrevista:

- ¿Qué datos sensibles son manejados por el sistema?
- ¿Qué protección se les da a los datos del sistema?

En base a la información obtenida a través de la entrevista realizada el día 09/06/2016, se determinó que no se implementan controles extras (como ser controles criptográficos) para proteger aquellos datos manejados por el sistema que se consideran de gran importancia para la institución. Actualmente todos los datos del sistema son protegidos de la misma forma (restricción de acceso a los mismos, protección de la red del sistema a través de un firewall), independientemente de la importancia que estos tengan.

Se determinó además que los datos de mayor importancia manejados por el sistema son los datos relacionados a la historia clínica y los datos financieros.

#### **4.7.2.3.1 Consideraciones de control**

Debido a que el sistema actual no se extiende más allá de la institución, ni tampoco establece comunicaciones con otros sistemas, consideramos que los riesgos de seguridad a los que actualmente está expuesto son riesgos relacionados al mal uso del sistema (errores causados por el mal manejo del mismo, accesos no autorizados causados por el mal uso de contraseñas). Es por esto que consideramos que los métodos que actualmente se utilizan para proteger el sistema y a la integridad de los datos del mismo (Firewall, control de acceso al sistema) son adecuados.

Recomendamos que se consideren las soluciones propuestas en **4.5.4.1.1** (código malicioso), **4.6.3.1.1** (uso de contraseñas), **4.6.3.2.1** (Equipamiento de usuario que se deja desatendido), **4.6.5.1.1** (Procedimientos seguros de inicio de sesión). Estas soluciones ayudan a proteger el sistema contra accesos no autorizados que puedan afectar la integridad de los datos manejados por el sistema

#### **4.7.2.4 Validación de los datos de salida**

### **Control**

*“Se recomienda que se valide la salida de datos de una aplicación para garantizar que el procesamiento de la información almacenada sea correcto y adecuado a las circunstancias ”<sup>169</sup>*

### **Relevamiento**

---

<sup>168</sup> IRAM-ISO/IEC 27002:2008

<sup>169</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

Con el propósito de examinar el cumplimiento del presente control, se realizó una entrevista al Jefe del Sector de Sistemas Informáticos, dado que, es este sector el encargado de la administración y el mantenimiento de los sistemas informáticos.

De acuerdo a lo establecido en el control “Validación de los datos de salida” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:

- ¿Los datos de salida son validados mediante controles específicos?
- ¿Qué controles se aplican?

En base a la información obtenida en la entrevista realizada el día 09/06/2016, se determinó que, con el objetivo de garantizar que los datos entregados por el sistema sean correctos, en primera instancia se establecen controles para garantizar que los datos cargados al sistema sean correctos y en segunda instancia, el sistema provee al usuario información suficiente para que este pueda determinar que los datos devueltos por el sistema son adecuados (En la emisión de reportes se provee de una pre-visualización antes de emitir el documento). Más allá de lo detallado previamente no se aplican controles extras que garanticen que los datos procesados y devueltos por el sistema sean correctos. Es por esto que consideramos que el presente control se cumple parcialmente dentro de la institución.

#### 4.7.2.4.1 Cambios recomendados

Consideramos que los controles aplicados actualmente al sistema para validar que los datos de salida, si tenemos en cuenta el tamaño de la organización y la cantidad de personal que hacen uso del sistema, son adecuados. Sin embargo, con el objetivo de ampliar estos controles y garantizar un correcto cumplimiento del presente control dentro de la organización, recomendamos que, al igual que se recomendó con la validación de los datos de entrada, se elabore un documento en donde se indiquen las responsabilidades por la validación de los datos de aquellas personas que hacen uso del sistema. Dicho documento debe tener como principal premisa concientizar a los usuarios sobre la importancia de verificar que los datos devueltos por el sistema sean correctos y de reportar cualquier error de estos, para que, después de una adecuada investigación y evaluación, estos sean corregidos. Este documento debe ser elaborado por el comité de seguridad de la información y aprobado por la gerencia.

#### 4.7.3 Controles criptográficos

*“Objetivo: Proteger la confidencialidad, autenticidad, y la integridad de la información por medios criptográficos.*

*Es conveniente desarrollar una política en el uso de controles criptográficos. Se recomienda que se establezca a gestión de claves para dar soporte al uso de técnicas criptográficas.”<sup>170</sup>*

##### 4.7.3.1 Política de utilización de controles criptográficos y gestión de claves

#### **Controles**

*“Se recomienda desarrollar e implementar una política para el uso de controles criptográficos para la protección de la información”<sup>171</sup>*

---

<sup>170</sup> IRAM-ISO/IEC 27002:2008

<sup>171</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

*“Se recomienda que se establezca la gestión de claves para dar soporte al uso organizacional de técnicas criptográficas”<sup>172</sup>*

### **Relevamiento**

Con el fin de corroborar el cumplimiento del presente control en el hospital se realizó una entrevista con el jefe del sector de sistemas informáticos, ya que, de existir controles criptográficos para proteger la información, el sector tendría conocimiento sobre los mismos.

En base a lo establecido en los controles *“Política de utilización de controles criptográficos”* y *“Gestión de claves”* de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:

- ¿En la institución se aplican controles criptográficos?
- ¿Existe una política para el uso de controles criptográficos?
- ¿Cuáles son los puntos tratados en la política para el uso de controles criptográficos?
- ¿Las claves criptográficas están protegidas de toda modificación, pérdida o destrucción?
- ¿Se protege físicamente al equipo utilizado para generar, almacenar y archivar claves?
- ¿De qué manera se gestionan las claves criptográficas? ¿Qué normas/procedimientos existen para esto?

A través de la entrevista realizada el día 09/06/2016, se determinó que en la institución no se aplican controles criptográficos, razón por la cual no fue posible realizar un adecuado estudio y análisis del presente control.

#### **4.7.3.1.1 Consideraciones de control**

Si se considera la aplicación de controles criptográficos para proteger la información en diferentes casos (protección de medios removibles, protección de contraseñas, protección de registros de auditorías), recomendamos la elaboración de una política de utilización de controles criptográficos. Proponemos que para esto se considere adaptar, según las necesidades de la institución, la política propuesta por la ONTI. A continuación, se detalla la misma:

*“El Organismo establece la presente Política de uso de controles criptográficos, a fin de Determinar su correcto uso. Para ello se indica que:*

- a) *Se utilizarán controles criptográficos en los siguientes casos:*
  - 1. *Para la protección de claves de acceso a sistemas, datos y servicios.*
  - 2. *Para la transmisión de información clasificada, fuera del ámbito del Organismo.*
  - 3. *Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Responsable de Seguridad Informática.*
- b) *Se desarrollarán procedimientos respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.*
- c) *El Responsable del Área Informática propondrá la siguiente asignación de funciones:*

---

<sup>172</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

| <i>Función</i>                                                   | <i>Cargo</i> |
|------------------------------------------------------------------|--------------|
| <i>Implementación de la Política de Controles Criptográficos</i> |              |
| <i>Administración de Claves</i>                                  |              |

d) Se utilizarán los siguientes algoritmos de cifrado y tamaños de clave:

*Cifrado Simétrico*

| <i>Algoritmo</i> | <i>Longitud de Clave</i> |
|------------------|--------------------------|
| <i>AES</i>       | <i>128/192/256</i>       |
| <i>3DES</i>      | <i>168 bits</i>          |
| <i>IDEA</i>      | <i>128 bits</i>          |
| <i>RC4</i>       | <i>128 bits</i>          |
| <i>RC2</i>       | <i>128 bits</i>          |

*Cifrado Asimétrico*

| <i>Casos de utilización</i>                                                                                                                                  | <i>Algoritmo</i> | <i>Longitud de clave</i> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|--------------------------|
| <i>Para certificados utilizados en servicios relacionados a la firma digital (sellado de tiempo, almacenamiento seguro de documentos electrónicos, etc.)</i> | <i>RSA</i>       | <i>2048 bits</i>         |
|                                                                                                                                                              | <i>DSA</i>       | <i>2048 bits</i>         |
|                                                                                                                                                              | <i>ECDSA</i>     | <i>210 bits</i>          |
| <i>Para certificados de sitio seguro</i>                                                                                                                     | <i>RSA</i>       | <i>1024 bits</i>         |
| <i>Para certificados de Certificador o de información de estado de certificados</i>                                                                          | <i>RSA</i>       | <i>2048 bits</i>         |
|                                                                                                                                                              | <i>DSA</i>       | <i>2048 bits</i>         |
|                                                                                                                                                              | <i>ECDSA</i>     | <i>210 bits</i>          |
|                                                                                                                                                              | <i>RSA</i>       | <i>1024 bits</i>         |

|                                                             |       |           |
|-------------------------------------------------------------|-------|-----------|
| Para certificados de usuario (personas físicas o jurídicas) | DSA   | 1024 bits |
| Para digesto seguro                                         | ECDSA | 160 bits  |
|                                                             | SHA-1 | 256 bits  |

Los algoritmos y longitudes de clave mencionados son los que a la fecha se consideran seguros. Se recomienda verificar esta condición periódicamente con el objeto de efectuar las actualizaciones correspondientes.

#### e) Cifrado

Mediante la evaluación de riesgos que llevará a cabo el Propietario de la Información y el Responsable de Seguridad Informática, se identificará el nivel requerido de protección, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.”<sup>173</sup>

Por otro lado, recomendamos, establecer normas y controles para una adecuada gestión de las claves criptográficas. Para esto recomendamos adaptar, según sea necesario, lo propuesto por la ONTI. A continuación, se detalla esto:

#### “Protección de Claves Criptográficas

Se implementará un sistema de administración de claves criptográficas para respaldar la utilización por parte del Organismo de los dos tipos de técnicas criptográficas, a saber:

- Técnicas de clave secreta (criptografía simétrica), cuando dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla.
- Técnicas de clave pública (criptografía asimétrica), cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar y una clave privada (que debe mantenerse en secreto) utilizada para descifrar. Las claves asimétricas utilizadas para cifrado no deben ser las mismas que se utilizan para firmar digitalmente.

Todas las claves serán protegidas contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.

Se aplicarán con éste propósito los algoritmos criptográficos enumerados en el punto anteriormente.

Se proporcionará una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.

#### Normas, Procedimientos y Métodos

<sup>173</sup> Oficina Nacional de Tecnologías de la Información. 2005. Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional. [http://www.sgp.gov.ar/sitio/PSI\\_Modelo-v1\\_200507.pdf](http://www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf). Página vigente al 17/11/2015

Yustman, Mauricio Ezequiel

*Se redactarán las normas y procedimientos necesarios para:*

- a. Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.*
- b. Generar y obtener certificados de clave pública de manera segura.*
- c. Distribuir claves de forma segura a los usuarios que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban.*
- d. Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.*
- e. Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.*
- f. Revocar claves, incluyendo cómo deben retirarse o desactivarse las mismas, por ejemplo, cuando las claves están comprometidas o cuando un usuario se desvincula del Organismo (en cuyo caso las claves también deben archivarse).*
- g. Recuperar claves perdidas o alteradas como parte de la administración de la continuidad de las actividades del Organismo, por ejemplo, para la recuperación de la información cifrada.*
- h. Archivar claves, por ejemplo, para la información archivada o resguardada.*
- i. Destruir claves.*
- j. Registrar y auditar las actividades relativas a la administración de claves.*

*A fin de reducir la probabilidad de compromiso, las claves tendrán fechas de inicio y caducidad de vigencia, definidas de manera que sólo puedan ser utilizadas por el lapso de (indicar lapso no mayor a 12 meses).*

*Además de la administración segura de las claves secretas y privadas, deberá tenerse en cuenta la protección de las claves públicas. Este problema es abordado mediante el uso de un certificado de clave pública. Este certificado se generará de forma que vincule de manera única la información relativa al propietario del par de claves pública/privada con la clave pública.*

*En consecuencia, es importante que el proceso de administración de los certificados de clave pública sea absolutamente confiable. Este proceso es llevado a cabo por una entidad denominada Autoridad de Certificación (AC) o Certificador.”<sup>174</sup>*

Es importante aclarar que, tanto la política de utilización de controles criptográficos, como las normas para la adecuada gestión de las claves criptográficas, deben ser elaboradas por el responsable de la seguridad de la información y aprobadas por el comité de seguridad de la información y por la gerencia.

#### 4.7.4 Seguridad de los archivos de sistema

*“Objetivo: Garantizar la seguridad de los archivos de sistema.*

*Se recomienda que se controle el acceso a los archivos del sistema y al código fuente del programa, y que los proyectos de tecnología de información y las actividades de soporte*

---

<sup>174</sup> Oficina Nacional de Tecnologías de la Información. 2005. Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional. [http://www.sgp.gov.ar/sitio/PSI\\_Modelo-v1\\_200507.pdf](http://www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf). Página vigente al 17/11/2015

se conduzcan de manera segura. Es conveniente tener cuidado para evitar la exposición de los datos sensibles en el ambiente de pruebas.”<sup>175</sup>

#### 4.7.4.1 Control del software operacional

##### **Control**

“Es conveniente que existan procedimientos para controlar la instalación de software en sistemas operacionales”<sup>176</sup>

##### **Relevamiento**

Con el objeto de examinar el cumplimiento del presente control en la organización, y en base a lo establecido en el control “Control de software operacional” de la norma IRAM-ISO/IEC 27002:2008, se utilizaron las siguientes técnicas de recopilación de datos:

- **Entrevista:** De acuerdo a lo establecido en el control “Control de software operacional” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:
  - ¿De qué manera son controlados los cambios en los sistemas operacionales?
  - Los cambios/actualizaciones de sistemas operativos de las instalaciones de procesamiento de la información ¿De qué manera son manejados?
  - ¿Quiénes están autorizados para poder hacer estos cambios?
  - ¿Existe software operacional provisto por terceros? ¿Existe soporte por parte de terceros?
- **Análisis de documentación:** Se procedió a realizar un análisis del documento “Normativas para el uso de recursos informáticos”, el cual se encuentra en el anexo apartado 7.1

Conforme a los datos obtenidos a través de la entrevista realizada el día 09/06/2016 y del análisis de la documentación previamente mencionada, se completó el siguiente Checklist:

| Control de software operacional                                                                                         | Sí | No |
|-------------------------------------------------------------------------------------------------------------------------|----|----|
| ¿Existe software de terceros en las áreas bajo estudio?                                                                 |    | X  |
| Se tienen en cuenta las siguientes directrices para controlar cambios en los sistemas operacionales:                    |    |    |
| La actualización del software operacional, aplicaciones y bibliotecas de programas solo la realizan los administradores | X  |    |
| Los sistemas operacionales solo guardan código ejecutable aprobado (no código en desarrollo o compiladores)             | X  |    |
| El software de aplicaciones se implementan luego de una prueba exitosa                                                  | X  |    |

<sup>175</sup> IRAM-ISO/IEC 27002:2008

<sup>176</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

|                                                                                                                  |   |   |
|------------------------------------------------------------------------------------------------------------------|---|---|
| Se lleva registro de todo el software implementado y su correspondiente documentación                            |   | X |
| Establecer una adecuada estrategia de vuelta atrás antes de implementar cambios                                  | X |   |
| Registro de todas las actualizaciones                                                                            |   | X |
| Almacenar versiones previas del software (junto a toda la información necesaria) como una medida de contingencia | X |   |

Tabla 4.7-3

Cómo es posible apreciar en el checklist, se pudo determinar que todo cambio en los equipos de procesamiento de la información (actualización de software, instalación de nuevas aplicaciones, etc.) es realizado por el personal de sistemas informáticos de la institución, ya que estos están adecuadamente capacitados y autorizados para realizarlo. Esto se indica en la “*Normativas para el uso de recursos informáticos*”, allí se detalla claramente que solo el personal de sistemas informáticos puede realizar estos tipos de cambios. Por otro lado, debido a la naturaleza (cliente-servidor) del sistema ERP que posee la institución, las estaciones de trabajo no poseen código en desarrollo o compiladores (todas las herramientas de desarrollo sólo son accesibles por el personal autorizado del sector de informática). Así mismo, como se menciona en 4.5.1.2 (gestión de cambios), todas las actualizaciones del sistema se implementan luego de una adecuada prueba y se establecen medidas (backup) para volver al estado previo a la actualización. Es importante aclarar que, las actualizaciones al firewall se realizan de igual manera, en primera instancia se realizan copias de seguridad y luego se verifica en otro ambiente que la actualización se realice adecuadamente (sin errores y completa) para, una vez comprobado su adecuado funcionamiento, actualizar en el ambiente operativo. Por último, tal cual se detalla en el último punto del checklist, se realizan copias de seguridad de versiones previas del software (principalmente del sistema ERP y del firewall), sin embargo, estas copias no almacenan documentación referente al software, por lo cual consideramos que este último punto se cumple parcialmente.

Es necesario aclarar que no se llevan registros de todas las actualizaciones realizadas, ni tampoco de todo el software implementado con su correspondiente documentación. Es por esto que concluimos que el presente control se cumple parcialmente dentro de la institución.

#### 4.7.4.1.1 Cambios recomendados

Con el objetivo de cumplimentar con todos los puntos propuestos por el control bajo estudio, recomendamos se consideren las siguientes directrices:

- Llevar un registro de todas las actualizaciones/cambios realizados al sistema ERP de la institución. Es recomendable que dicho registro contenga información referente a: tipo de cambio, módulos afectados, fecha del cambio, nombre del backup realizado previo a la implementación, responsable del cambio. Este registro debe contener toda la información que se considere adecuada.
- Almacenar las copias de seguridad de los sistemas (sistema ERP y firewall) junto con toda la documentación correspondiente (detalles de configuración, código, parámetros, etc.)

Es adecuado que una persona determinada sea la encargada de implementar todo cambio en el software, es por esto que recomendamos asignar esta responsabilidad a una persona determinada del sector de sistemas informáticos. Esta persona debe encargarse de coordinar que la implementación de todo cambio en el software se realice con éxito y sin provocar dificultades en el trabajo diario de los usuarios.

#### 4.7.4.2 Protección de los datos de prueba del sistema

##### **Control**

*“Es conveniente que se seleccionen cuidadosamente, se protejan y controlen los datos de prueba.”<sup>177</sup>*

##### **Relevamiento**

Con el propósito de verificar el cumplimiento del presente control, se realizó una entrevista al jefe del sector de sistemas informáticos, ya que este sector es el responsable del cuidado de los datos de prueba del sistema. A partir de lo establecido por el control “Protección de los datos de prueba del sistema” de la norma IRAM-ISO/IEC 27002:2008, se realizaron las siguientes preguntas:

- ¿Se emplean los datos operacionales del sistema de producción para propósitos de prueba? En caso afirmativo ¿Los datos sensibles son modificados o eliminados antes de hacer uso de los mismos?
- En el entorno de prueba ¿Se emplean los mismos métodos de acceso que para los sistemas operacionales?
- ¿Existen autorizaciones formales y particulares por cada vez que los datos operativos son copiados a los entornos de prueba?
- ¿Los datos operativos son eliminados una vez completada la prueba en los sistemas de aplicación de prueba?
- ¿Se registra la copia y uso de los datos operativos en los entornos de prueba para auditorías posteriores?

En base a la información obtenida, el día 09/06/2016, se completó el siguiente Checklist:

| Protección de los datos de prueba del sistema                                                                                                   | Sí | No |
|-------------------------------------------------------------------------------------------------------------------------------------------------|----|----|
| Los datos operacionales de la organización no son empleados para propósitos de prueba                                                           |    | X  |
| Los datos sensibles provenientes de las bases de datos operacionales son modificados o eliminados, para que sean irreconocibles antes de su uso |    | X  |
| Para proteger los datos operacionales, en los entornos de prueba, se aplican las siguientes directrices:                                        |    |    |
| Se aplican los mismos procedimientos de control de acceso en los sistemas de prueba y en los de producción                                      | X  |    |
| Existen autorizaciones formales y particulares por cada vez que los datos operativos son copiados a los entornos de prueba                      |    | X  |

<sup>177</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

|                                                                                                                             |  |   |
|-----------------------------------------------------------------------------------------------------------------------------|--|---|
| La información operativa es borrada de los entornos de prueba inmediatamente luego de concluida la prueba                   |  | X |
| Se lleva un registro de la copia y el uso de la información operativa en los entornos de prueba para posteriores auditorías |  | X |

Tabla 4.7-4

Como puede verse en el Checklist, y tal como se establece en **4.5.1.4** (Separación de las instalaciones de desarrollo, de pruebas y operacionales), los datos de la base de producción son copiados por completo a la base de datos de prueba, y la información sensible no es alterada de ninguna forma ni eliminada para que los mismos sean irreconocibles. A pesar de esto, en los entornos de prueba, se aplican los mismos métodos de control de acceso, por lo que, en este caso, se cumplimenta con este punto del presente control. En cuanto a los puntos restantes, ninguno de ellos es aplicado dentro de la organización, por lo que, consideramos que no se cumplimenta con el presente control.

#### 4.7.4.2.1 Cambios Recomendados

Recomendamos que, para lograr el cumplimiento del control, debe implementarse la solución propuesta en **4.5.1.4.1** (Separación de las instalaciones de desarrollo, de pruebas y operacionales), donde se establece que debe crearse una base de datos de prueba, lo más próxima a la realidad para evitar la copia o el traspaso de los datos operacionales al ambiente de pruebas. De esta manera, se lograría cumplimentar lo establecido por el control “*Protección de los datos de prueba del sistema*”.

#### 4.7.4.3 Control de acceso al código fuente de programa

##### **Control**

*“Se recomienda que se restrinja el acceso al código fuente de programa”<sup>178</sup>*

##### **Relevamiento**

Con el propósito de verificar el cumplimiento del presente control, se realizó una entrevista al jefe del sector de sistemas informáticos, ya que este sector es el responsable del resguardo del código fuente de programa. A partir de lo establecido por el control “*Control de acceso al código fuente de programa*” de la norma IRAM-ISO/IEC 27002:2008, se realizaron las siguientes preguntas:

- ¿Los códigos fuente de los programas y librerías se mantienen en los sistemas operacionales (en el ambiente de producción)?
- ¿Existen procedimientos formales (o informales) para gestionar el código fuente y las bibliotecas de código? ¿En qué consisten estos procedimientos?
- ¿El personal de soporte dispone de acceso irrestricto al código fuente y a las bibliotecas?
- ¿Se otorga autorización previa para realizar actualizaciones al código fuente y bibliotecas?
- ¿La documentación de programas se almacenan en un ambiente seguro?
- ¿Se mantiene un registro de auditoría de todos los accesos a las bibliotecas y código fuente?

<sup>178</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

- ¿El mantenimiento y copia de las bibliotecas y código fuente se encuentran sujetas a un procedimiento estricto de control de cambios?

Conforme a los datos obtenidos durante el relevamiento, realizado el día 09/06/2016, se completó el siguiente Checklist:

| Control de acceso al código del programa                                                       | Sí | No |
|------------------------------------------------------------------------------------------------|----|----|
| Para controlar el acceso al código fuente del programa                                         |    |    |
| Las bibliotecas y el código fuente no se mantienen en los sistemas operacionales               |    | X  |
| El código fuente y las librerías se gestionan en base a un procedimiento determinado           |    | X  |
| El personal de soporte no tiene acceso total al código fuente y las librerías                  |    | X  |
| Las actualizaciones sobre el código fuente y las librerías se realizan con previa autorización |    | X  |
| La documentación del sistema se almacena en un sitio seguro                                    | X  |    |
| Existen registros de auditoría que contienen los accesos a las bibliotecas del programa fuente |    | X  |
| Existen procedimientos estrictos de control de cambios para el código fuente y librerías       |    | X  |

Tabla 4.7-5

Puede observarse en el Checklist anterior que las bibliotecas de programa y el código fuente se mantienen en el ambiente de producción, lo cual se debe a que, al emplear un lenguaje de programación interpretado, es necesario para el funcionamiento del sistema, mantener el código fuente en los ambientes de producción. Así mismo, no se dispone de ningún procedimiento formal para gestionar el código fuente y las librerías, ni para su control de cambios, y, además, el personal del sector dispone de acceso irrestricto a las mismas. Tampoco existen registros de auditoría que contienen los accesos a las bibliotecas ni al código fuente.

Finalmente, es necesario aclarar que la documentación del sistema se almacena en un sitio seguro, ya que, tal como se establece en **4.5.7.4** (Seguridad de la documentación del sistema), la misma se encuentra almacenada en un directorio especial al que solo dispone acceso el personal de Sistemas Informáticos, y, por lo tanto, este es el único punto que se cumplimenta adecuadamente.

Cabe destacar que, tal como se menciona en el “*Procedimiento de Gestión de Cambios*”, detallado en **4.5.1.2** (Gestión de cambios), al momento de implementar cambios sobre el sistema, se realiza un resguardo de la información y del sistema, es decir, del código fuente del mismo (al tratarse de un lenguaje interpretado), por lo que, se toman ciertas medidas para proteger el código y sus librerías. A pesar de esto, ya que el “*Procedimiento de Gestión de Cambios*” previamente mencionado no se encuentra formalizado, consideramos que no se cumplimenta con ningún punto adicional del presente control, a pesar de la medida informal anteriormente indicada.

#### 4.7.4.3.1 Consideraciones de control

Debido a que el personal del sector de Sistemas Informáticos es limitado, y los mismos cuentan con un gran número de tareas y responsabilidades bajo su cargo, consideramos que no es apropiado establecer controles especiales sobre el código fuente y las librerías de programas, ya que dichas medidas podrían entorpecer enormemente las tareas del personal sin aportar beneficios reales a la organización. Sin embargo, en caso que en el futuro se incorpore personal al sector, el presente control debe ser reevaluado para establecer una solución apropiada.

#### 4.7.5 Seguridad en los procesos de desarrollo y soporte

*“Objetivo: Mantener la seguridad del software y la información del sistema de aplicación*

*Se recomienda que se controlen estrictamente los ambientes de proyectos y de soporte.*

*Es conveniente que los gerentes responsables de los sistemas de aplicación también se responsabilicen de la seguridad del ambiente de proyecto o de soporte. Se recomienda que ellos garanticen la revisión de todos los cambios propuestos para el sistema, a fin de comprobar que no comprometen la seguridad del sistema o del ambiente operativo.”<sup>179</sup>*

##### 4.7.5.1 Procedimientos de control de cambios

#### **Control**

*“Es conveniente que la implementación de cambios se controle mediante el uso de procedimientos formales de control de cambios.”<sup>180</sup>*

#### **Relevamiento**

Para verificar lo establecido por el control “*Procedimientos de control de cambios*”, se procedió a evaluar su cumplimiento, según lo establecido en la norma IRAM-ISO/IEC 27002:2008, a través de las siguientes herramientas:

- Entrevista: debido a que la implementación de cambios a los sistemas existentes (o bien, nuevos sistemas) dentro de la organización depende del sector de Sistemas Informáticos, estimamos conveniente la realización de una entrevista con el jefe de dicho sector, para lo cual se elaboraron las siguientes preguntas
  - En la introducción de sistemas o cambios en el existente ¿Se sigue un proceso formal de documentación, especificación, pruebas, control de calidad, e implementación?
  - ¿Se realiza una evaluación de riesgos, un análisis de impactos de los cambios y se establecen los controles de seguridad necesarios a implementar? ¿Se toman las debidas precauciones para que no se alteren los procesos y controles de seguridad existentes?
  - ¿Se garantiza los programadores solo tengan acceso a aquellas partes del sistema que necesitan para desempeñar sus tareas?
  - ¿Existe algún registro que contiene los niveles de autorización acordados con el responsable de los datos?

---

<sup>179</sup> IRAM-ISO/IEC 27002:2008

<sup>180</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

- ¿Se identifican todos los activos (hardware, bases de datos o aplicaciones, por ejemplo) que requieran correcciones?
  - ¿Se actualiza la documentación del sistema, una vez implementados los cambios? ¿Qué documentación es actualizada?
  - ¿Se mantiene un versionado del sistema?
  - ¿Se planifica previamente en qué momento y en qué lugar se implementarán los cambios?
- Análisis del “Proceso de Gestión de Cambios”, mencionado en 4.5.1.2 (Gestión de cambios), ya que en el mismo se establece de qué manera se gestionan los cambios sobre los sistemas de la organización

Conforme a los datos obtenidos durante la entrevista realizada al jefe del sector de sistemas informáticos, realizada el día 09/06/2016, se completó el siguiente Checklist:

| Procedimientos de control de cambios                                                                                                                    | Sí | No |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|
| Existe un proceso formal de control de cambios                                                                                                          |    | X  |
| El proceso de control de cambios contempla:                                                                                                             |    |    |
| Documentación de cambios/sistema                                                                                                                        |    | X  |
| Especificación de cambios/sistema                                                                                                                       | X  |    |
| Pruebas                                                                                                                                                 | X  |    |
| Control de Calidad                                                                                                                                      | X  |    |
| Implementación                                                                                                                                          | X  |    |
| Se realiza una evaluación de riesgos antes de la implementación del cambio                                                                              |    | X  |
| Se analizan los impactos de los cambios sobre la infraestructura y sistemas existentes                                                                  | X  |    |
| Se establecen los controles de seguridad a aplicar                                                                                                      | X  |    |
| Se toman medidas para evitar la alteración de controles de seguridad existentes                                                                         |    | X  |
| Se establecen controles para lograr que los programadores tengan acceso únicamente a aquellas partes del sistema que requieren para realizar sus tareas |    | X  |
| Se obtiene una aprobación formal de una autoridad para la implementación de los cambios                                                                 |    | X  |
| El procedimiento de Control de Cambios incluye:                                                                                                         |    |    |
| El mantenimiento de un registro de los niveles de autorización acordados                                                                                |    | X  |
| Garantías que los cambios son propuestos por usuarios autorizados                                                                                       | X  |    |

|                                                                                                                                                          |   |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|
| Controles que permiten evitar que los cambios comprometan procedimientos de seguridad                                                                    |   | X |
| Identificación de todos los activos que requieran correcciones                                                                                           |   | X |
| Aprobación formal de los cambios antes de iniciar las tareas                                                                                             |   | X |
| Garantías de que los usuarios autorizados aprueban los cambios antes de su implementación                                                                | X |   |
| Garantías que la documentación del sistema se encuentra actualizada                                                                                      |   | X |
| Mantenimiento de un control de versiones                                                                                                                 |   | X |
| Mantenimiento de una huella de auditoría de todas las solicitudes de cambio                                                                              |   | X |
| Garantías que los procesos operativos y los manuales de usuario se modifiquen y se mantengan actualizados                                                |   | X |
| Garantías que la implementación de los cambios se realice en el lugar y momento adecuados para no entorpecer el funcionamiento normal de la organización | X |   |

Tabla 4.7-6

Como puede verse en el Checklist anterior, no existe un proceso formal de control de cambios dentro de la organización, sin embargo, en análisis anteriores, específicamente en **4.5.1.2** (Gestión de cambios), se determinó que existe un proceso informal para gestionar cambios en los sistemas e instalaciones de procesamiento de la información. Tal como se explica en el control mencionado anteriormente, el mismo contempla la especificación, pruebas, control de calidad e implementación, en las etapas de “*Elaboración de Cambios*”, “*Prueba de validación*” e “*Implementación*” respectivamente. Cabe destacar que la mayoría de las veces no se elabora documentación del sistema, y en aquellos casos en los que se dispone de documentación, la misma no se actualiza debidamente ante un cambio en las funcionalidades del sistema.

Por otra parte, no se realiza una evaluación de riesgos antes de la implementación de los cambios, pero si se analizan los impactos de los cambios sobre la actual infraestructura y sistema para determinar la viabilidad del cambio, durante la etapa “*Evaluación de Cambio*”, y también se determinan, de manera informal, los controles de seguridad a aplicar (por ejemplo, que usuario tendrá acceso a los datos, quienes podrán modificarlos o eliminarlos, etc.) durante la etapa de “*Elaboración de Cambios*”.

En cuanto a las medidas que se aplican para evitar la alteración de controles de seguridad y los controles para evitar que los programadores dispongan de un acceso irrestricto al sistema, dichas medidas no se aplican dentro de la organización, y tal como se establece en **4.5.1.2** (Gestión de cambios), tampoco se obtiene una aprobación formal por parte de una autoridad al momento de implementar un cambio, aunque es necesario aclarar que si se obtiene una aprobación informal para realizar este proceso.

Finalmente, el proceso de gestión de cambios ofrece garantías que los cambios son propuestos por usuarios autorizados, ya que, antes de comenzar con su planificación, se solicita una autorización (informal) al responsable de los datos (por lo general, el jefe del sector o programa involucrado), con lo cual se garantiza que dicho usuario se encuentra autorizado para solicitar el cambio; en cuanto a las garantías que los cambios se realicen en el lugar y momento apropiado, el sector de sistemas informáticos consulta al programa/sector involucrado cual es el momento oportuno en el cual pueden implementarse los cambios, y se establece una fecha precisa para realizar esta operación para no entorpecer el trabajo de los usuarios. También, debe aclararse que existen garantías que los cambios son autorizados por los usuarios, ya que, antes de implementarse los mismos, los usuarios realizan pruebas de validación para confirmar que los mismos satisfacen sus necesidades.

En cuanto a los puntos restantes del control, no se cumplimenta adecuadamente con ninguno de los mismos, ya que no se lleva un versionado de los cambios realizados sobre el ERP “Open Source” utilizado. Además, la documentación, cuando se encuentra disponible, no suele actualizarse. Tampoco existen controles especiales para evitar que los cambios comprometan controles de seguridad existentes, ni se mantiene una huella de auditoría de los cambios.

#### 4.7.5.1.1 Cambios Recomendados

A través de los cambios propuestos en 4.5.1.2.1 (Gestión de cambios), se lograría formalizar un proceso para controlar los cambios en el sistema del Hospital, y se realizaría una evaluación de los riesgos de seguridad implicados junto con el análisis de impacto sobre el sistema y la infraestructura existente.

#### 4.7.5.2 Revisiones técnicas de las aplicaciones luego de cambios en el sistema operativo

##### **Control**

*“Cuando se realizan cambios en los sistemas operativos, se recomienda que se revisen y prueben las aplicaciones críticas del negocio para garantizar que no se produzca un impacto adverso en las operaciones o la seguridad organizacionales.”<sup>181</sup>*

##### **Relevamiento**

Con el fin de corroborar el cumplimiento del presente control en el hospital se realizó una entrevista con el jefe del sector de sistemas informáticos, ya que, el mantenimiento, actualización y cambio de los sistemas operativos dentro de la organización son tareas propias del sector mencionado anteriormente.

Durante la entrevista se realizaron las siguientes preguntas, en base a lo establecido en el control “Revisiones técnicas de las aplicaciones luego de cambios en el sistema operativo” de la norma IRAM-ISO/IEC 27002:2008:

- ¿Se sigue un procedimiento formal o informal para la implementación de cambios en los sistemas operativos? ¿En qué consiste el mismo?
- ¿Se revisa que las aplicaciones no hayan sido comprometidas por estos cambios?

---

<sup>181</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

En base a la información obtenida durante la entrevista, realizada el día 09/06/2016, se determinó la existencia de un proceso informal para la gestión de cambios en los sistemas operativos, el cual exponemos a continuación:



Ilustración 4.7-1

- I. Revisar actualizaciones disponibles: De manera periódica, se comprueban las actualizaciones disponibles para el sistema operativo del Servidor. Esta actividad es llevada a cabo por el jefe del Sector de Sistemas Informáticos. Cabe destacar que no existe un tiempo determinado tras el cual se comprueba la existencia de actualizaciones.
- II. Instalación y Configuración en el Ambiente de Prueba: En caso de existir una actualización disponible, se procede a instalar y configurar la misma, en el ambiente de prueba.
- III. Testeo en el Ambiente de Prueba: Una vez finalizada la instalación y configuración de la actualización, se procede a realizar testeos sobre el ambiente de prueba, con el objeto de determinar si existen conflictos con los sistemas operacionales. En caso de existir, las actualizaciones no son instaladas en el ambiente de producción.
- IV. Actualización en Ambiente de Producción: Finalmente, las actualizaciones son instaladas y configuradas en el Ambiente productivo.

En base a la información detallada anteriormente se procedió a verificar el cumplimiento de lo establecido en el presente control, mediante el siguiente Checklist:

|                                                                                                                                            |    |    |
|--------------------------------------------------------------------------------------------------------------------------------------------|----|----|
| Revisiones técnicas de las aplicaciones luego de cambios en el sistema operativo                                                           | Sí | No |
| Existe un procedimiento (formal o informal) para gestionar cambios en los sistemas operativos                                              | X  |    |
| El procedimiento contempla los siguientes puntos:                                                                                          |    |    |
| La revisión y control de aplicaciones para garantizar que no se encuentren comprometidas por los cambios del sistema operativo             | X  |    |
| El presupuesto anual contempla los costos de las revisiones y pruebas del sistema como consecuencia de los cambios en el sistema operativo |    | X  |

|                                                                                                                                                             |   |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---|--|
| Los cambios sobre el Sistema Operativo son notificados en tiempo, para que puedan llevarse las pruebas y revisiones antes que los mismos sean implementados | X |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|---|--|

Tabla 4.7-7

Tal como puede verse en el Checklist, existe un procedimiento informal para gestionar los cambios en los sistemas operativos. Sin embargo, cabe destacar que el mismo solo aplica al Sistema Operativo del servidor. Podemos observar que dicho proceso verifica que las aplicaciones no se encuentren comprometidas por los cambios del sistema operativo, lo cual es realizado en el paso “*Testeo en el Ambiente de Prueba*”, y consideramos que los cambios son notificados en tiempo, debido a que se revisan periódicamente la existencia de actualizaciones, a pesar de no existir un tiempo determinado para estas revisiones.

En el caso de los equipos de tipo cliente, no existe un proceso formal para gestionar cambios sobre los mismos. Cabe destacar que, cuando se emplea un nuevo sistema operativo, previamente se verifica que el sistema ERP funcione sobre el mismo. Consideramos que, debido a la arquitectura del sistema ERP, la verificación realizada es suficiente para la organización.

#### 4.7.5.2.1 Cambios Recomendados

Consideramos que, para cumplimentar con lo establecido en el presente control, es necesario formalizar el proceso de gestión de cambios sobre el sistema operativo, debiéndose establecer un tiempo determinado tras el cual se verifique la existencia de actualizaciones. Esta tarea debe ser realizada por el jefe del Sector de Sistemas Informáticos.

#### 4.7.5.2.2 Consideraciones de control

En el caso que se considere necesario, o bien, si en el futuro es imprescindible validar el correcto funcionamiento de las actualizaciones en los equipos cliente, es recomendable la instalación y configuración del servicio “*WSUS*” (Windows Server Update Services), en el servidor en el que se encuentra instalado el “*Controlador de Dominio*” propuesto en (Procedimientos seguros de Inicio de Sesión **4.6.5.1**). A través del mismo, es posible gestionar de manera efectiva las actualizaciones de los sistemas operativos de tipo “*cliente*”. Cabe destacar que, en este caso, será necesario:

- Establecer políticas de grupo en el “*controlador de dominio*” para habilitar en los equipos de tipo cliente las actualizaciones automáticas.
- Establecer políticas de grupo en el “*controlador de dominio*” para que los equipos clientes realicen la búsqueda de actualizaciones en el Servidor donde se encuentra instalado el servicio de actualizaciones de Windows (WSUS), previamente mencionado.
- Formalizar y adoptar el procedimiento “*Proceso de Gestión de cambios en el SO*”, mencionado al inicio del presente control, para gestionar las actualizaciones de los sistemas operativos en los equipos de tipo cliente. Se debe tener en cuenta que:
  - Para la instalación en el ambiente de prueba, es posible aprobar todas las actualizaciones disponibles para un grupo determinado de usuarios (en este caso, los usuarios del sector de Sistemas Informáticos) para realizar las pruebas necesarias.
  - “*WSUS*” permite gestionar de manera individual cada una de las actualizaciones distribuidas, permitiendo aprobar, rechazar o incluso indicar a las estaciones de

trabajo que deben desinstalar una determinada actualización. De esta manera, es posible aprobar, al momento de realizar el despliegue de las actualizaciones en el ambiente de producción, únicamente aquellas actualizaciones que no generan ningún tipo de conflicto con los sistemas existentes.

#### 4.7.5.3 Restricción de cambio en los paquetes de software

##### **Control**

*“Es conveniente que se desalienten las modificaciones a los paquetes de software y se limiten a los cambios necesarios. Se recomienda que se controlen estrictamente todos los cambios.”<sup>182</sup>*

##### **Relevamiento**

Con el objeto de examinar el cumplimiento del presente control en la organización, se realizó una entrevista al jefe del sector de sistemas informáticos, debido a que es responsabilidad de dicho sector la implementación de cambios sobre los paquetes de software utilizados.

En base a lo establecido en el control “Restricción de cambio en los paquetes de software” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:

- ¿Se realizan modificaciones sobre los paquetes de software suministrados por terceras partes?
- ¿Se tienen en cuenta los riesgos de que se comprometan los procesos de integridad y controles incorporados en estos paquetes?
- ¿Se obtiene el consentimiento de la tercera parte para realizar estos cambios?
- ¿Existe la posibilidad que la tercera parte provea los cambios requeridos sobre los paquetes de software en forma de actualizaciones?
- ¿Se tienen en cuenta los costos del mantenimiento futuro por los cambios implementados?
- ¿Se mantiene una copia del software original? ¿Los cambios se implementan sobre una copia claramente identificada, luego de realizar la instalación de todos los parches y actualizaciones aprobadas?
- ¿Los cambios son claramente documentados?
- ¿Un evaluador independiente realiza las pruebas de validación de los cambios realizados?

En base a la información obtenida durante la entrevista, realizada el día 09/06/2016, se procedió a completar el siguiente Checklist:

| Restricción de cambio en los paquetes de software                                         | Sí | No |
|-------------------------------------------------------------------------------------------|----|----|
| Los paquetes de software proporcionados por terceras partes se emplean sin modificaciones |    | X  |

<sup>182</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

|                                                                                                                              |   |   |
|------------------------------------------------------------------------------------------------------------------------------|---|---|
| Se tienen en cuenta los riesgos implicados en la modificación de los paquetes de software proporcionados por terceras partes |   | X |
| Se obtiene el consentimiento del proveedor para modificar estos paquetes de software                                         | X |   |
| Es posible obtener los cambios requeridos a través de la tercera parte en forma de actualizaciones                           |   | X |
| Se consideran los costos de mantenimiento futuro del software por los cambios implementados                                  |   | X |
| Se mantiene una copia de seguridad del software original                                                                     | X |   |
| Los cambios son implementados en una copia claramente identificada, luego de aplicados todos los parches y actualizaciones   | X |   |
| Los cambios se documentan claramente                                                                                         |   | X |

Tabla 4.7-8

Puede verse en el Checklist anterior, que los paquetes de software provistos por terceras partes son modificados. Esto se debe a que, actualmente, la organización emplea un sistema ERP de tipo “*Open Source*”, el cual fue desarrollado por un tercero, y sobre el cual se realizaron las modificaciones necesarias para adaptarlo al Hospital, y por esta razón, consideramos que este sistema en sí es un paquete de software provisto por una tercera parte. A pesar de esto, debe aclararse que no existe un tercero que realice tareas de desarrollo o de mantenimiento sobre este sistema, sino que estas tareas son desarrolladas por el personal del sector. Al tratarse de un software de código abierto, se dispone de la autorización para realizar modificaciones al código del mismo, lo cual se encuentra establecido por escrito en la licencia GNU del mismo. Por otra parte, se mantienen copias de seguridad con el software sin las modificaciones implementadas, y tal como se establece en **4.5.1.2** (Gestión de cambios), al momento de implementar cambios, se guarda un respaldo completo del sistema antes de implementarlos, de manera que pueda recuperarse la última versión estable del sistema, en caso que los cambios antes mencionados provoquen un mal funcionamiento del sistema. En consecuencia, consideramos que los cambios son implementados sobre una copia del sistema, sobre el cual se aplicaron previamente todos los parches y actualizaciones de sistema.

Sin embargo, cabe destacar que no se evalúan los posibles riesgos de modificar el software provisto por la tercera parte, y es necesario aclarar que no pueden obtenerse los cambios por parte del tercero, debido a que actualmente el software empleado se encuentra desatendido por parte de sus desarrolladores (la versión del software con la que se trabaja es antigua). Tampoco se consideran los posibles costos de mantenimiento futuro, debido a que, actualmente el sector de Sistemas Informáticos es el único encargado de realizar el mantenimiento de dicho sistema, y no existen terceras partes a las cuales se les realice un pago por mantenimiento. En cuanto a la documentación de los cambios, tal como se menciona en Gestión del cambio, normalmente (cuando se dispone de documentación) la misma no es debidamente actualizada.

#### 4.7.5.3.1 Cambios Recomendados

A pesar que consideramos que el sistema ERP en sí constituye un paquete de software provisto por una tercera parte, es necesario mencionar que también se encuentra sujeto a los procesos de gestión y control de cambio (ver gestión de cambios y Gestión de cambio en los servicios de terceras partes) y consideramos que, con las soluciones propuestas en los controles mencionados se alcanzaría un nivel de cumplimiento adecuado en el presente control.

#### 4.7.5.4 Fuga de información

##### **Control**

*“Se recomienda que se prevengan las oportunidades de fuga de la información.”<sup>183</sup>*

##### **Relevamiento**

Con el propósito de examinar el cumplimiento del presente control, se realizó una entrevista al Jefe del Sector de sistemas informáticos, dado que, es este sector el responsable del monitoreo del uso del sistema y de la implementación de técnicas, métodos o herramientas que permitan proteger el flujo de información del sistema.

De acuerdo a lo establecido en el control “*Fuga de Información*” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:

- ¿Existen controles que permitan detectar o descubrir la fuga de información dentro de la organización (monitoreo de las comunicaciones, uso de software especial, seguimiento de las actividades del personal, seguimiento del uso de recursos informáticos)?

Conforme a los datos obtenidos durante la entrevista realizada el día 09/06/2016, se completó el siguiente Checklist:

| Fuga de Información                                             | Sí | No |
|-----------------------------------------------------------------|----|----|
| Para limitar el riesgo de fuga de la información:               |    |    |
| Se monitorean las comunicaciones en busca de información oculta |    | X  |
| Se monitorea el uso del sistema                                 |    | X  |
| Se monitorea la actividad del personal                          |    | X  |
| Seguimiento del uso de otros recursos informáticos              |    | X  |

Tabla 4.7-9

Tal como se indica en el Checklist anterior, no se aplican controles especiales para reducir el riesgo de fuga de información en la organización.

Cabe destacar que, aunque se disponen de logs de auditoría que permiten controlar las operaciones de los usuarios, y de ciertas herramientas para el monitoreo de sus actividades (ver **4.5.10.1** “registros de auditoría” y **4.5.10.2** “seguimiento del uso del sistema”), sin embargo, es necesario aclarar que los mismos no suelen emplearse ni revisarse, debido a la falta de recursos en el sector de Sistemas Informáticos. Por otro lado, tal como se establece en **4.5.6.1** Control

<sup>183</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

de redes, no existe una persona que se dedica exclusivamente al monitoreo de las comunicaciones dentro de la organización.

#### 4.7.5.4.1 Cambios Recomendados

Consideramos que, entre las obligaciones del responsable de la seguridad de la información debe incluirse el monitoreo del uso del sistema y de las comunicaciones de la organización, de manera que sea posible reducir los riesgos de fuga de la información. En este caso, para el seguimiento y control de las comunicaciones de red, es necesario en primer lugar implementar la solución propuesta en 4.5.4.1.1 (Controles contra código malicioso), de manera que el responsable de seguridad disponga de las herramientas apropiadas para esta tarea.

Estimamos que la solución propuesta es suficiente para la organización, debido a que no se trata de una organización de grandes dimensiones.

#### 4.7.5.5 Desarrollo tercerizado de software

##### **Control**

*“Se recomienda que la organización supervise, siga y controle el desarrollo externo de software.”<sup>184</sup>*

##### **Relevamiento**

Con el fin de corroborar el cumplimiento del presente control en el hospital se realizó una entrevista con el jefe del sector de sistemas informáticos, ya que, es responsabilidad del sector el control y supervisión del desarrollo de software realizado por terceras partes.

Durante la entrevista se realizaron las siguientes preguntas, en base a lo establecido en el control “*Desarrollo tercerizado de software*” de la norma IRAM-ISO/IEC 27002:2008:

- ¿Existen terceras partes que desarrollan software para la organización?
- ¿Existen acuerdos de licencia, de propiedad de código o de derechos de propiedad intelectual entre el Hospital y estos terceros?
- ¿De qué manera se evalúa la calidad y precisión del trabajo llevado a cabo?
- ¿Existen acuerdos de custodia (“*escrow*”) entre el Hospital y la tercera parte?
- ¿La tercera parte otorga derechos de acceso para auditar la calidad del software construido y el trabajo realizado?
- ¿En el contrato se establecen los requerimientos de calidad y seguridad que debe cumplir el software desarrollado por la tercera parte?
- ¿Se realizan pruebas sobre el código, antes de la instalación, para detectar la existencia código malicioso?

En base a la información obtenida durante la entrevista, realizada el día 09/06/2016, se procedió a completar el siguiente Checklist:

| Desarrollo tercerizado de software                                                     | Sí | No |
|----------------------------------------------------------------------------------------|----|----|
| Para el desarrollo tercerizado de software, se tienen en cuenta los siguientes puntos: |    |    |
| Acuerdos de licencia, propiedad de código o de propiedad intelectual                   |    | X  |

<sup>184</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

|                                                                                |  |   |
|--------------------------------------------------------------------------------|--|---|
| Certificación de la calidad y precisión del trabajo desarrollado               |  | X |
| Acuerdos de custodia (o “escrow”)                                              |  | X |
| Derechos de acceso para auditar la calidad y el trabajo realizado              |  | X |
| Requerimientos contractuales con respecto a la calidad y a la seguridad        |  | X |
| Realización de pruebas antes de la instalación, para detectar código malicioso |  | X |

Tabla 4.7-10

Podemos observar en el Checklist anterior que no se cumplen ninguno de los puntos establecidos por el presente control. Esto se debe a que actualmente, existe un desarrollo tercerizado de software, pero el cual fue contratado por el Ministerio de Salud Pública de Salta, por lo que, el Hospital no dispone de la autoridad suficiente para alterar las condiciones contractuales bajo las cuales se contrataron a la tercera parte. En consecuencia, el caso no es el ideal para evaluar la validez del presente control, y por ello, se encuentra incluido dentro de las restricciones del presente proyecto.

Por otra parte, tal como se menciona en **4.7.5.3** (Restricción de Cambio en los paquetes de software), el sistema ERP actual del Hospital consiste en un enlatado de código abierto, provisto por una tercera parte, que fue modificado para adaptarlo a las necesidades del Hospital por el personal del sector de Sistemas Informáticos. Cabe destacar que existe un acuerdo de licencia entre el tercero y el Hospital, el cual es un acuerdo GNU (o GPL por sus siglas en inglés), a través del cual el tercero otorga a la organización la libertad de usar, estudiar, compartir (copiar) y modificar el software. A pesar de esto, estimamos que este no es el caso ideal para evaluar los puntos mencionados en el presente control, debido a que la tercera parte no fue contratada por la Institución para desarrollar el software actual, sino que el mismo fue empleado como base, por el personal del sector de Sistemas Informáticos, para construir el Sistema vigente.

Consideramos que actualmente, no existe un caso válido sobre el cual evaluar el cumplimiento del presente control.

#### 4.7.5.5.1 Consideraciones de control

En el futuro, en caso que se decida tercerizar el desarrollo de software dentro de la organización, es primordial que el contrato elaborado entre el Hospital y la tercera parte incluya cláusulas referentes a:

- Acuerdos de licencia, de propiedad del código creado o de propiedad intelectual del software construido.
- Requerimientos en cuanto a la calidad del software y a su seguridad. Para ello, es útil establecer cuáles son los tiempos de respuesta esperados, y las pruebas de seguridad que debe superar el sistema, por ejemplo.
- El derecho acceso, por parte del Hospital, al código y trabajo realizado por la tercera parte para supervisar el trabajo realizado, y la obligación de esta última de proveer los canales y herramientas necesarias para realizar esta tarea.

Consideramos que las cláusulas que hacen referencia a los puntos anteriores deben ser elaboradas por el Comité de Seguridad de la Información y su inclusión en el contrato debe ser autorizada por la gerencia del Hospital.

#### 4.7.6 Gestión de Vulnerabilidades técnicas

*“Objetivo: Reducir el riesgo resultante de la explotación de vulnerabilidades técnicas publicadas.*

*Se recomienda que la gestión de las vulnerabilidades técnicas se implemente en una forma efectiva, sistemática y repetible, con mediciones que confirmen su efectividad. Es conveniente que estas consideraciones incluyan a los sistemas operativos, y cualquier otra aplicación en uso.”<sup>185</sup>*

##### 4.7.6.1 Control de las vulnerabilidades técnicas

###### **Control**

*“Se recomienda que se obtenga información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información que son utilizados, que se evalúe la exposición de la organización a tales vulnerabilidades, y que se tomen las medidas adecuadas para tratar los riesgos asociados.”<sup>186</sup>*

###### **Relevamiento**

Para verificar el cumplimiento del presente control dentro de la organización se procedió a realizar una entrevista al Jefe del Sector de Sistemas Informáticos, ya que, el desarrollo y prueba de los sistemas de información es tarea de dicho sector.

Teniendo en cuenta lo establecido en el control “Control de las vulnerabilidades técnicas” de la norma IRAM-ISO/IEC 27002:2008, se elaboraron las siguientes preguntas a realizar durante la entrevista:

- ¿Existen procedimientos (formales o informales) para detectar y gestionar las vulnerabilidades técnicas del software existente dentro de la organización?
- ¿Se establecen roles para gestionar las vulnerabilidades técnicas? (Seguimiento, análisis de riesgo, parcheo, rastreo activo, etc.)
- ¿Se identifican cuáles son los recursos (por ejemplo, software) empleados para identificar vulnerabilidades técnicas en los sistemas del Hospital?
- ¿Se establecen períodos para reaccionar cuando una vulnerabilidad es notificada o descubierta?
- ¿Se identifican los riesgos y las acciones a ser llevadas a cabo para corregir una vulnerabilidad cuando esta es descubierta/notificada?
- ¿La vulnerabilidad es manejada como un cambio en el sistema o como si se tratara de un incidente de seguridad de la información dependiendo de su urgencia?
- Si existe un parche para corregir la vulnerabilidad ¿Se evalúan los riesgos de instalar el parche? ¿Se prueban los mismos antes de instalarlos para garantizar que son efectivos?
- ¿Se mantienen registros de auditoría de las vulnerabilidades técnicas encontradas y de qué manera fueron resueltas?

---

<sup>185</sup> IRAM-ISO/IEC 27002:2008

<sup>186</sup> IRAM-ISO/IEC 27002:2008

Yustman, Mauricio Ezequiel

- ¿Se atienden primero los sistemas de alto riesgo?

A través de la entrevista realizada el día 09/06/2016 y considerando la información obtenida en la misma, se completó el siguiente Checklist:

| Control de las vulnerabilidades técnicas                                                                                            | Sí | No |
|-------------------------------------------------------------------------------------------------------------------------------------|----|----|
| Existen procedimientos que permiten detectar vulnerabilidades técnicas en los sistemas de la organización                           |    | X  |
| Se establecen roles y responsabilidades para la gestión de vulnerabilidades técnicas                                                |    | X  |
| Se identifican las herramientas tecnológicas empleadas para buscar vulnerabilidades técnicas relevantes en los sistemas             |    | X  |
| Se establecen períodos para reaccionar ante las notificaciones de vulnerabilidades técnicas                                         |    | X  |
| Se identifican los riesgos y las acciones a ser llevadas a cabo una vez identificada una vulnerabilidad técnica                     |    | X  |
| Las vulnerabilidades son atendidas a través del proceso de gestión de cambios o como un incidente de la seguridad de la información |    | X  |
| En caso de existir un parche, se evalúan los riesgos de su instalación                                                              |    | X  |
| Los parches son probados y evaluados antes de su instalación para garantizar que son efectivos                                      |    | X  |
| Se mantiene un registro de auditoría para todos los procedimientos emprendidos                                                      |    | X  |
| Los sistemas de alto riesgo se atienden primero                                                                                     |    | X  |

Tabla 4.7-11

Puede observarse en el Checklist anterior que no existen procedimientos dentro de la organización que permitan identificar vulnerabilidades técnicas para su corrección, y, en consecuencia, no se cumplen los puntos establecidos por el presente control. Cabe destacar que, cuando surgen actualizaciones, ya sea para el Firewall de la institución, o para el Sistema Operativo del servidor, las mismas son aplicadas luego de ser testeadas en ambientes de prueba para verificar que funcionen correctamente y que no generan conflictos o mal funcionamiento en la infraestructura tecnológica. Sin embargo, cabe destacar que no se realiza ningún tipo de evaluación de los riesgos de la instalación de los parches, ni se evalúa si los mismos resuelven las vulnerabilidades que, en teoría, los mismos deberían resolver, o bien si generan nuevas vulnerabilidades en la infraestructura tecnológica de la organización.

#### 4.7.6.1.1 Cambios Recomendados

Recomendamos que la detección e identificación de vulnerabilidades técnicas se encuentre a cargo del responsable de la seguridad de la Información dentro de la organización. Para ello, existen una serie de herramientas, que permiten asistirlo en esta tarea, entre las cuales podemos mencionar las siguientes:

- QUALYS Browser Check: Herramienta que permite realizar un análisis de los navegadores y “plugins” instalados, con el fin de detectar vulnerabilidades en los mismos.
- Rapid7 NEXPOSE: Software que permite identificar vulnerabilidades de los sistemas operativos y bases de datos existentes dentro de la organización. El mismo dispone de una versión gratuita que permite realizar el escaneo de hasta 32 direcciones IP diferentes.
- RETINA: Similar a Rapid7 NEXPOSE, pero que dispone de una versión gratuita que permite escanear hasta 256 direcciones IP distintas.
- Matriux: Es una distribución de seguridad que dispone de un gran número de herramientas de código abierto para realizar test de penetración, hacking ético, pruebas de seguridad, análisis de seguridad y hacking ético, entre otros.

Cabe destacar que estas herramientas deben ser registradas en el inventario de activos de la organización.

Una vez detectada una vulnerabilidad, es recomendable que sea atendida a través del proceso de gestión de cambios o a través de la gestión de incidentes, dependiendo de su gravedad.

Consideramos que, dada la magnitud de la organización, y a los recursos disponibles, la solución propuesta es suficiente.

#### 4.7.6.1.2 Consideraciones de control

Con el propósito de realizar una verificación más detallada, recomendamos se considere la realización de auditorías de seguridad externas. Para esto recomendamos la contratación de servicios de “hacking ético”. Este servicio permitirá a la institución comprobar la existencia de vulnerabilidades de seguridad, para posteriormente a través de un informe, revelar aquellos fallos de seguridad encontrados, mitigarlos a la brevedad posible y evitar fugas de información y ataques informáticos.

Al momento de contratar este tipo de servicio deben considerarse algunos aspectos de gran importancia:

- Acuerdo de confidencialidad: es importante establecer un acuerdo de confidencialidad entre la institución y la empresa encargada de brindar este tipo de servicio, para así resguardar la información confidencial/sensible involucrada en el proceso y también para proteger la información resultante referente a las vulnerabilidades detectadas.
- Experiencia y trayectoria: es importante tener en cuenta la experiencia comprobable de la empresa a contratar, así como también considerar la trayectoria de la misma en el rubro.
- Establecer de manera clara los puntos que serán evaluados: Es necesario establecer de manera precisa los aspectos que serán testeados por la empresa en cuestión.
- Clausulas referentes al resarcimiento en caso de daño a la información: Es importante establecer clausulas para proteger la información que pueda ser dañada y aclarar la responsabilidad de la empresa en este aspecto.

#### 4.7.7 Plan de trabajo

##### 4.7.7.1 Requisitos previos

Serán requisitos previos para la implementación de las soluciones propuestas:

- La existencia del rol de responsable de seguridad de la información dentro de la institución (tal como se menciona en **4.1.1.3**(política de seguridad)).
- La existencia del Comité de Seguridad de la Información (tal como se menciona en **4.2.1.2.1**(Coordinación de la Seguridad)).
- La existencia de una Política de Seguridad en el Hospital (ver **4.1.1.3**(política de seguridad)).
- La existencia de un inventario de Información (ver **4.3.1.1.1** (inventario de información)).
- La existencia de un proceso de gestión de cambio (ver **4.5.1.2.1** (**Gestión de cambios**)).

##### 4.7.7.2 WBS (estructura de desglose de trabajo)

A continuación, se establecen las actividades a llevar a cabo para implementar las soluciones propuestas en el presente control.

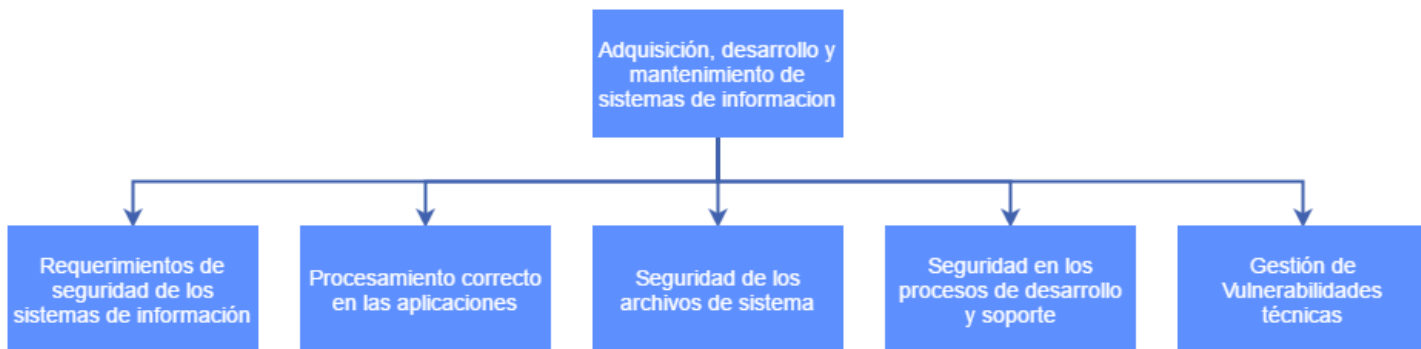


Ilustración 4.7-2

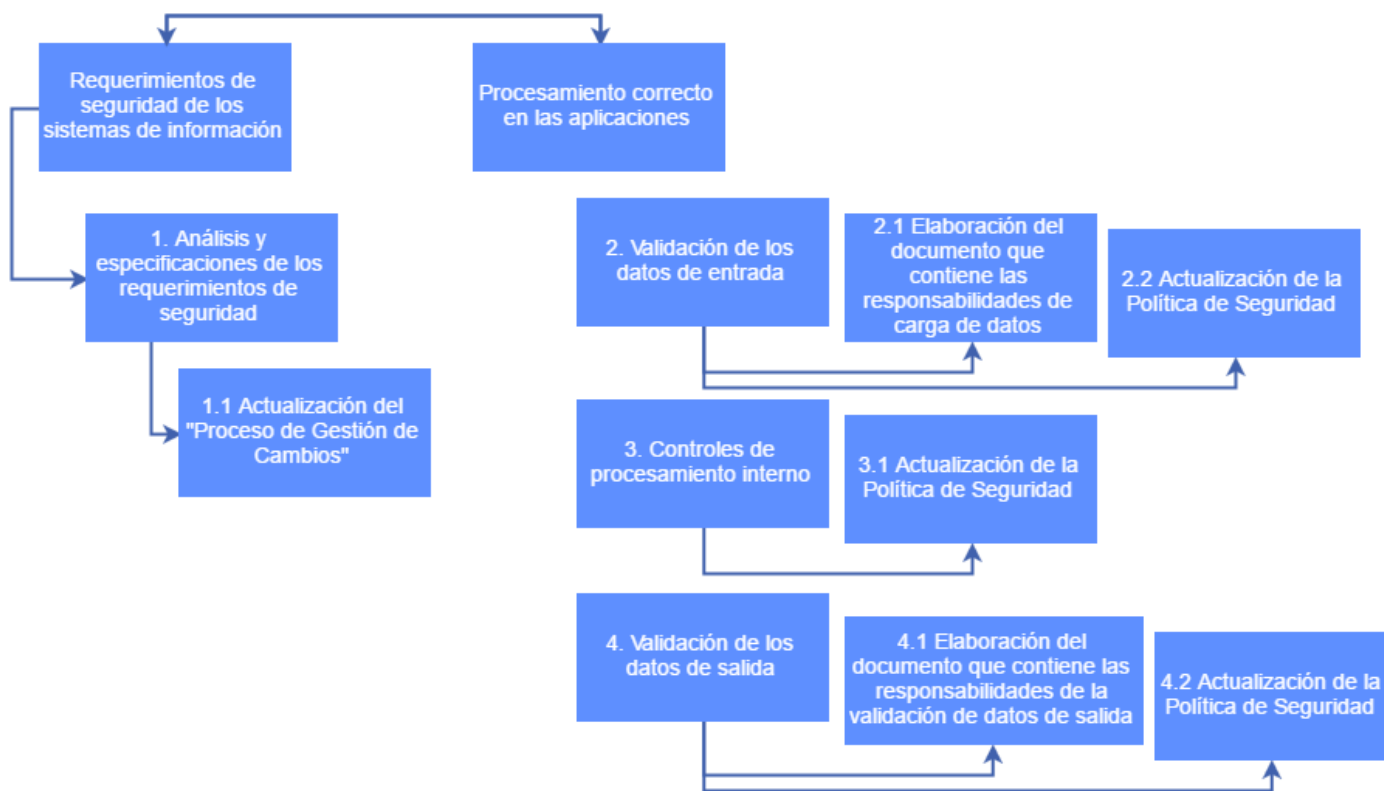


Ilustración 4.7-3

## **Requerimientos de seguridad de los sistemas de información**

### **1. Análisis y especificaciones de los requerimientos de seguridad**

1.1. Actualización del "Proceso de Gestión de Cambios": Se actualizan las tareas a realizar en la etapa de "Evaluación de cambios" del proceso en cuestión.

## **Procesamiento correcto en las aplicaciones**

### **2. Validación de los datos de entrada**

2.1. Elaboración del documento que contiene las responsabilidades de carga de datos: se procede a elaborar un documento en el cual se detallen las responsabilidades del usuario encargado de realizar carga de datos al sistema de la institución

2.2. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Validación de los datos de entrada) trabajada

### **3. Controles de procesamiento interno**

3.1. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Controles de procesamiento interno) trabajada

### **4. Validación de los datos de salida**

- 4.1. Elaboración del documento que contiene las responsabilidades de la validación de datos de salida: se procede a elaborar un documento en el cual se detallen las responsabilidades en la verificación de la salida de los datos de aquellos usuarios que hacen uso del mismo.
- 4.2. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Validación de los datos de salida) trabajada

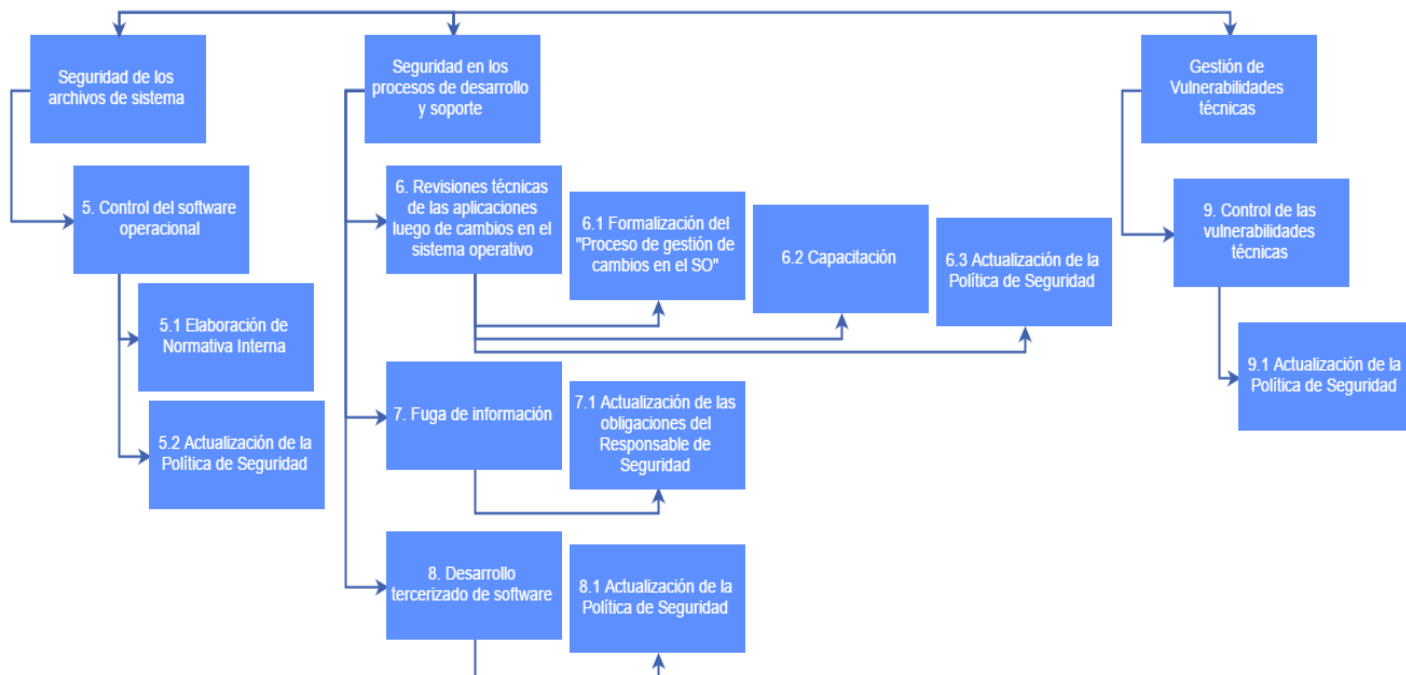


Ilustración 4.7-4

### **Seguridad de los archivos de sistema**

#### **5. Control del software operacional.**

- 5.1. Elaboración de Normativa Interna: Se procede a elaborar una normativa interna para regular la manera que deben de realizarse los registros de las diferentes actualizaciones/cambios realizados al sistema.
- 5.2. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Control del software operacional) trabajada

### **Seguridad en los procesos de desarrollo y soporte**

#### **6. Revisiones técnicas de las aplicaciones luego de cambios en el sistema operativo**

- 6.1. Formalización del "Proceso de gestión de cambios en el SO": se procede a documentar y detallar el proceso de autorización para instalaciones de procesamiento de la información teniendo en cuenta todas las modificaciones/mejoras que deben ser consideradas aplicar al mismo. Posteriormente, dicho proceso es evaluado y aprobado. Finalmente, el mismo es distribuido al personal que corresponda
- 6.2. Capacitación: se capacita al personal involucrado en el proceso con el propósito de que las tareas sean realizadas conforme a lo establecido previamente.

6.3. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Revisiones técnicas de las aplicaciones luego de cambios en el sistema operativo) trabajada

7. Fuga de información

7.1. Actualización de las obligaciones del Responsable de Seguridad: Se procede a ampliar las obligaciones del responsable de seguridad de la información, de manera tal que éstas incluyan las obligaciones de monitoreo y control de la infraestructura tecnológica de la institución.

8. Desarrollo tercerizado de software

8.1. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Desarrollo tercerizado de software) trabajada.

**Gestión de Vulnerabilidades técnicas**

9. Control de las vulnerabilidades técnicas

9.1. Actualización de la Política de Seguridad: se procede a actualizar el capítulo correspondiente de la política de seguridad. Se incluye en la política de seguridad todas las pautas/lineamientos necesarios sobre la temática (Control de las vulnerabilidades técnicas.) trabajada

4.7.7.3 *Estimación de tiempos*

Seguidamente, se establecen los tiempos y recursos para cada una de las actividades previamente detalladas

UCS - Facultad de Ingeniería  
Revisión de los Procesos de Seguridad del Hospital Dr. Arturo Oñativia  
Solución Propuesta

|    | Nombre                                                                                           | Duración | Predecesoras | Recursos                                   |
|----|--------------------------------------------------------------------------------------------------|----------|--------------|--------------------------------------------|
| 1  | Adquisición, desarrollo y mantenimiento de sistemas de información                               | 30d      |              |                                            |
| 2  | Inicio de tareas de Adquisición, Desarrollo y Mantenimiento de Sistemas de Inf                   | 0h       |              |                                            |
| 3  | Requerimientos de seguridad de los sistemas de información                                       | 0.5d     |              |                                            |
| 4  | Análisis y especificaciones de los requerimientos de seguridad                                   | 0.5d     |              |                                            |
| 5  | Actualización del 'Proceso de Gestión de Cambios'                                                | 3h       | 2            | Comité de Seguridad de la Información      |
| 6  | Procesamiento correcto en las aplicaciones                                                       | 27.17d   |              |                                            |
| 7  | Validación de los datos de entrada                                                               | 13.83d   |              |                                            |
| 8  | Elaboración del documento que contiene las responsabilidades de carga de datos                   | 12h      | 5            | Comité de Seguridad de la Información      |
| 9  | Actualización de la Política de Seguridad                                                        | 1h       | 8            | Responsable de Seguridad de la Información |
| 10 | Controles de procesamiento interno                                                               | 0.33d    |              |                                            |
| 11 | Actualización de la Política de Seguridad                                                        | 2h       | 9            | Responsable de Seguridad de la Información |
| 12 | Validación de los datos de salida                                                                | 13.83d   |              |                                            |
| 13 | Elaboración del documento que contiene las responsabilidades de la validación de datos de salida | 12h      | 8            | Comité de Seguridad de la Información      |
| 14 | Actualización de la Política de Seguridad                                                        | 3h       | 11,13        | Responsable de Seguridad de la Información |
| 15 | Seguridad de los archivos de sistema                                                             | 28.17d   |              |                                            |
| 16 | Control del software operacional                                                                 | 28.17d   |              |                                            |
| 17 | Elaboración de Normativa Interna                                                                 | 12h      | 2            | Jefe del Sector de Sistemas Informáticos   |
| 18 | Actualización de la Política de Seguridad                                                        | 3h       | 14,17        | Responsable de Seguridad de la Información |
| 19 | Seguridad en los procesos de desarrollo y soporte                                                | 27d      |              |                                            |
| 20 | Revisiones técnicas de las aplicaciones luego de cambios en el sistema operativo                 | 26.5d    |              |                                            |
| 21 | Formalización del 'Proceso de gestión de cambios en el SO'                                       | 6h       | 17           | Jefe del Sector de Sistemas Informáticos   |
| 22 | Capacitación                                                                                     | 2h       | 21           | Jefe del Sector de Sistemas Informáticos   |
| 23 | Actualización de la Política de Seguridad                                                        | 2h       | 18,22        | Responsable de Seguridad de la Información |
| 24 | Fuga de información                                                                              | 0.33d    |              |                                            |
| 25 | Actualización de las obligaciones del Responsable de Seguridad                                   | 3h       | 13           | Comité de Seguridad de la Información      |
| 26 | Desarrollo tercerizado de software                                                               | 0.5d     |              |                                            |
| 27 | Actualización de la Política de Seguridad                                                        | 3h       | 23           | Responsable de Seguridad de la Información |
| 28 | Gestión de Vulnerabilidades técnicas                                                             | 1d       |              |                                            |
| 29 | Control de las vulnerabilidades técnicas                                                         | 1d       |              |                                            |
| 30 | Actualización de la Política de Seguridad                                                        | 6h       | 27           | Responsable de Seguridad de la Información |
| 31 | Fin de tareas de Adquisición, Desarrollo y Mantenimiento de Sistemas de Inf                      | 0h       | 25,30        |                                            |

Ilustración 4.7-5

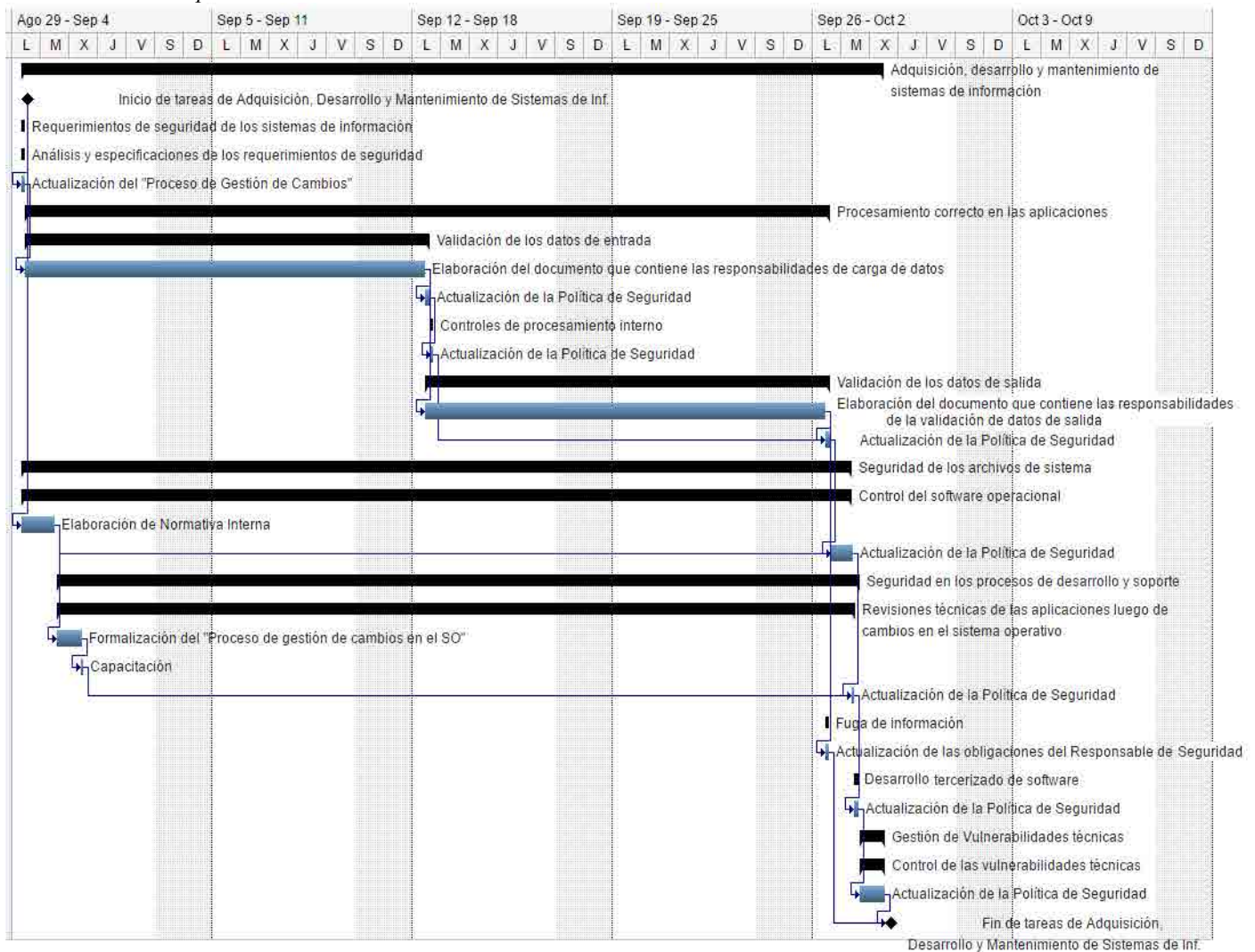


Ilustración 4.7-6

#### 4.7.8 Análisis de riesgos

Se establecen los riesgos a los que está expuesta la institución al no realizar una adecuada gestión de Adquisición, desarrollo y mantenimiento de sistemas de información.

| Riesgo                                                                                                                                      | Impacto         | Probabilidad      | Importancia       | Prevención                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b><u>Daño a la integridad de la información manejada por el sistema, debido a una inadecuada validación de carga y salida de datos</u></b> | <b><u>6</u></b> | <b><u>0,8</u></b> | <b><u>4,8</u></b> | <b><u>Adecuados controles de seguridad establecidos para el sistema.</u></b><br><br><b><u>responsabilidades definidas en la carga y validación de datos</u></b><br><br><b><u>Adecuada gestión del control de acceso</u></b> |

|                                                                                                                               |                  |                    |                   |                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------------|------------------|--------------------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b><u>Fuga de información, debido a la falta de monitoreo de sistema y de las comunicaciones y/o exploits del sistema</u></b> | <b><u>10</u></b> | <b><u>0,25</u></b> | <b><u>2,5</u></b> | <b><u>Monitoreo del uso del sistema y los sistemas de comunicación.</u></b><br><br><b><u>Protección de los datos de prueba del sistema</u></b><br><br><b><u>Aplicaciones de controles criptográficos en caso de ser necesario</u></b> |
| <b><u>Mal funcionamiento de la estructura tecnológica, debido a actualizaciones de SO mal gestionadas</u></b>                 | <b><u>2</u></b>  | <b><u>0,15</u></b> | <b><u>0,3</u></b> | <b><u>Adecuados procedimientos para el control de cambio en los Sistemas Operativos</u></b>                                                                                                                                           |

Tabla 4.7-12

#### 4.7.9 Análisis Económico-Financiero

##### 4.7.9.1 Análisis de costos

- Hardware: Debido a que no es necesaria la adquisición de hardware extra, ya que no se requiere nuevo equipamiento, no se registran costos en este concepto.
- Software: Debido a que no es necesaria la adquisición de software extra, ya que no se requieren nuevos programas o aplicaciones (las aplicaciones sugeridas son gratuitas), no se registran costos en este concepto.
- Recursos Humanos: Debido a que el personal de la Institución es el encargado de llevar adelante las tareas anteriormente mencionadas, no se registran costos en este concepto.

##### 4.7.9.2 Beneficios operativos

Llevar adelante los cambios recomendados en los controles previamente analizados, brindara a la institución los siguientes beneficios:

- Reducción de errores en los sistemas de información.
- Aumento en la seguridad de los sistemas de información disponible en la institución.

##### 4.7.9.3 Análisis Económico

En base a los riesgos definidos, identificamos y estimamos el valor de cada uno de los activos que pueden verse afectados por los mismos, para lo cual, consideramos el tiempo y los recursos que son necesarios invertir para recuperar o recrear el activo en cuestión:

| Amenazas                                                                                                                      | Activos                | Tiempo Estimado de Recuperación                                                                                         | Recursos                    | Tiempo Total | Salario por Hora <sup>187</sup> | Valor del Activo            |
|-------------------------------------------------------------------------------------------------------------------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------|-----------------------------|--------------|---------------------------------|-----------------------------|
| Daño a la integridad de la información manejada por el sistema, debido a una inadecuada validación de carga y salida de datos | Activo de Información  | 690 horas <sup>188</sup>                                                                                                | 1 persona                   | 690 horas    | \$133,00                        | \$91.770,00                 |
| Fuga de información, debido a la falta de monitoreo de sistema y de las comunicaciones y/o exploits del sistema               | Activo de Información  | **En caso de Fuga de Información, pueden existir costos legales, y puede ser necesario indemnizar a la persona afectada | -                           | -            | -                               | \$605.897,52 <sup>189</sup> |
| Mal funcionamiento de la estructura tecnológica, debido a actualizaciones de SO mal gestionadas                               | Activo de Software     | 6 horas <sup>190</sup>                                                                                                  | 1 persona                   | 6 horas      | \$133,00                        | \$798,00                    |
|                                                                                                                               | Activos de Información | 2 horas <sup>191</sup>                                                                                                  | 140 empleados (como mínimo) | 280 horas    | \$133,00                        | \$37.240,00                 |

Tabla 4.7-13

<sup>187</sup> Se utilizó un Salario mensual de \$16000 con 30 hs semanales de trabajo.

<sup>188</sup> Se estima un promedio de 3 horas por día para resolver problemas por datos mal ingresados, en un promedio de 230 días laborables por año.

<sup>189</sup> Se estima a partir de la fórmula de Vuotto, con  $n=23,5$  y  $a=48750$  (salario mensual de \$15.000 y un porcentaje de incapacidad de 0,25). Daño por la información filtrada.

<sup>190</sup> Tiempo aproximado en restaurar el servidor y el sistema ERP de la organización.

<sup>191</sup> Se estima el tiempo que tardará un empleado en cargar información generada durante las 6 horas que el sistema no se encontraba disponible.

Yustman, Mauricio Ezequiel

A continuación, calculamos la Expectativa de Pérdida Individual para cada uno de los activos identificados anteriormente:

| Activo                 | Amenaza                                                                                                                       | Valor del Activo | EF (Factor de Exposición) | SLE (Expectativa de Pérdida Individual) |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------|------------------|---------------------------|-----------------------------------------|
| Activo de Información  | Daño a la integridad de la información manejada por el sistema, debido a una inadecuada validación de carga y salida de datos | \$91.770,00      | 0,5                       | \$45.885,00                             |
| Activo de Información  | Fuga de información, debido a la falta de monitoreo de sistema y de las comunicaciones y/o exploits del sistema               | \$605.897,52     | 0,65                      | \$393.833,39                            |
| Activo de Software     | Mal funcionamiento de la estructura tecnológica, debido a actualizaciones de                                                  | \$798,00         | 0,5                       | \$399,00                                |
| Activos de Información | SO mal gestionadas                                                                                                            | \$37.240,00      | 0,5                       | \$18.620,00                             |

Tabla 4.7-14

Con el propósito de calcular la Expectativa de Pérdida Anual (ALE), se realizó una estimación de la Tasa de Ocurrencia Anualizada (ARO), debido a la inexistencia de datos históricos de incidentes de seguridad de la información dentro de la organización, y se obtuvieron los siguientes valores:

| Activo                | Amenaza                                                                                                                       | SLE (Expectativa de Pérdida Individual) | ARO (Tasa de Ocurrencia Anualizada) | ALE (Expectativa de Pérdida Anual) |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|-------------------------------------|------------------------------------|
| Activo de Información | Daño a la integridad de la información manejada por el sistema, debido a una inadecuada validación de carga y salida de datos | \$45.885,00                             | 0,8                                 | \$36.708,00                        |
| Activo de Información | Fuga de información, debido a la falta de monitoreo de sistema y de las comunicaciones y/o exploits del sistema               | \$393.833,39                            | 0,25                                | \$98.458,35                        |

|                        |                                                                                                 |             |      |                     |
|------------------------|-------------------------------------------------------------------------------------------------|-------------|------|---------------------|
| Activo de Software     | Mal funcionamiento de la estructura tecnológica, debido a actualizaciones de SO mal gestionadas | \$399,00    | 0,15 | \$59,85             |
| Activos de Información |                                                                                                 | \$18.620,00 | 0,15 | \$2.793,00          |
| <b>Total</b>           |                                                                                                 |             |      | <b>\$138.019,20</b> |

Tabla 4.7-15

Como podemos ver, el total obtenido en la tabla anterior constituye la pérdida anual de la organización por no llevar adelante una adecuada adquisición, desarrollo y mantenimiento de sistemas de información.

#### 4.8 Resumen General.

##### 4.8.1 Cronograma General de Tareas

A continuación, se muestra un cronograma general, en el cual es posible visualizar el tiempo total estimado para realizar la implementación de las soluciones propuestas en los capítulos anteriores.

|    | Nombre                                                             | Duración | Predecesoras |
|----|--------------------------------------------------------------------|----------|--------------|
| 1  | Resumen Gral. de Tareas                                            | 607d     |              |
| 2  | Inicio de Tareas                                                   | 0d       |              |
| 3  | Política de Seguridad                                              | 27d      | 2            |
| 4  | Organización de la Seguridad                                       | 68d      | 3            |
| 5  | Gestión de activos                                                 | 74d      | 4            |
| 6  | Seguridad de los Recursos Humanos                                  | 67d      | 5            |
| 7  | Gestión de las Comunicaciones y Operaciones                        | 236d     | 6            |
| 8  | Control de Accesos                                                 | 105d     | 7            |
| 9  | Adquisición, Desarrollo y Mantenimiento de Sistemas de Información | 30d      | 8            |
| 10 | Fin de Tareas                                                      | 0d       | 9            |

Ilustración 4.8-1



Ilustración 4.8-2

Podemos ver, en los gráficos anteriores, que el tiempo total para la implementación de las soluciones propuestas en el presente proyecto es de 2 años y 4 meses aproximadamente.

## 4.8.2 Análisis Económico-Financiero General

## 4.8.2.1 Costos

A continuación, se presentan los costos generales para la implementación de las soluciones propuestas en los capítulos anteriores, y los costos anuales de mantenimiento:

| Costos Totales                                                    |           |              |                  |              |                    |
|-------------------------------------------------------------------|-----------|--------------|------------------|--------------|--------------------|
| Control                                                           | Hardware  | Software     | Recursos Humanos | Equipamiento | Total              |
| Políticas de Seguridad                                            | \$ 0      | \$ 0         | \$ 0             | \$ 0         | \$ 0               |
| Organización de la Seguridad                                      | \$ 0      | \$ 0         | \$ 0             | \$ 0         | \$ 0               |
| Gestión de Activos                                                | \$ 0      | \$ 0         | \$ 0             | \$ 0         | \$ 0               |
| Seguridad de los Recursos Humanos                                 | \$ 0      | \$ 0         | \$ 0             | \$ 0         | \$ 0               |
| Gestión de Comunicaciones y Operaciones                           | \$ 3.000  | \$ 0         | \$ 0             | \$ 13.000    | \$ 16.000          |
| Control de Accesos                                                | \$ 30.000 | \$ 88.438,40 | \$ 0             | \$ 0         | \$ 118.438,4       |
| Adquisición Desarrollo y Mantenimiento de Sistemas de Información | \$ 0      | \$ 0         | \$ 0             | \$ 0         | \$ 0               |
| <b>Total</b>                                                      |           |              |                  |              | <b>\$134.438,4</b> |

Tabla 4.8-1

| Costos Anuales               |          |          |                  |              |            |
|------------------------------|----------|----------|------------------|--------------|------------|
| Control                      | Hardware | Software | Recursos Humanos | Equipamiento | Total      |
| Políticas de Seguridad       | \$ 0     | \$ 0     | \$ 264.000       | \$ 0         | \$ 264.000 |
| Organización de la Seguridad | \$ 0     | \$ 0     | \$ 0             | \$ 0         | \$ 0       |

|                                                                   |      |              |      |      |                    |
|-------------------------------------------------------------------|------|--------------|------|------|--------------------|
| Gestión de Activos                                                | \$ 0 | \$ 0         | \$ 0 | \$ 0 | \$ 0               |
| Seguridad de los Recursos Humanos                                 | \$ 0 | \$ 0         | \$ 0 | \$ 0 | \$ 0               |
| Gestión de Comunicaciones y Operaciones                           | \$ 0 | \$ 45.827,60 | \$ 0 | \$ 0 | \$ 45.827,60       |
| Control de Accesos                                                | \$ 0 | \$ 0         | \$ 0 | \$ 0 | \$ 0               |
| Adquisición Desarrollo y Mantenimiento de Sistemas de Información | \$ 0 | \$ 0         | \$ 0 | \$ 0 | \$ 0               |
| <b>Total</b>                                                      |      |              |      |      | <b>\$309.827,6</b> |

Tabla 4.8-2

Podemos ver en las tablas anteriores que, para la implementación de las soluciones propuesta, se requiere una inversión total de \$134.438,4 para la adquisición del software, hardware y equipamiento extra necesario. Además, se requerirá la inversión de \$309.827,6 anuales aproximadamente para el mantenimiento anual de las licencias de software (antivirus) y los recursos humanos solicitados.

Es necesario que la organización realice un análisis de factibilidad económica, con el fin de determinar si es posible afrontar los costos que conlleva la implementación y el mantenimiento de las soluciones propuestas. Debido a que no se dispone de un acceso a dicha información, no es posible realizar dicho análisis en el presente proyecto.

#### 4.8.2.2 Análisis Económico

Finalmente, se presenta la Expectativa de Pérdida Anual para cada uno de los controles desarrollados, los cuales constituyen el ahorro, expresados en términos monetarios, que la organización podría alcanzar, en caso de implementar las soluciones propuestas a lo largo del presente proyecto:

| Control                                 | Expectativa de Pérdida Anual (ALE) |
|-----------------------------------------|------------------------------------|
| Organización de la Seguridad            | \$120.613,15                       |
| Gestión de Activos                      | \$103.350,10                       |
| Seguridad de los Recursos Humanos       | \$132.364,80                       |
| Gestión de Comunicaciones y Operaciones | \$475.338,89                       |

|                                                                   |                        |
|-------------------------------------------------------------------|------------------------|
| Control de Accesos                                                | \$132.474,12           |
| Adquisición Desarrollo y Mantenimiento de Sistemas de Información | \$138.019,20           |
| <b>Total</b>                                                      | <b>\$ 1.102.160,26</b> |

Tabla 4.8-3

Si comparamos el total obtenido anteriormente con los costos anuales de mantenimiento, detallados en la sección anterior, obtendremos el beneficio anual, cuantificado en términos monetarios, que la organización puede alcanzar en caso de implementar las soluciones propuestas a lo largo del presente proyecto.

| ITEM                               | Total                |
|------------------------------------|----------------------|
| Expectativa de Pérdida Anual (ALE) | \$ 1.102.160,26      |
| Costos Anuales                     | \$ 309.827,6         |
| <b>Total</b>                       | <b>\$ 792.332,66</b> |

Tabla 4.8-4

Finalmente, tal como puede observarse en la tabla anterior, es posible para la organización alcanzar un ahorro neto de \$ 792.332,66 anuales.

#### 4.9 Prototipo para la gestión de los incidentes de la seguridad de la información.

A diferencia del estudio realizado en los anteriores procesos de control, en el presente control, se procederá a elaborar un **PROTOTIPO** funcional de software con el objetivo de establecer una solución acorde a lo detallado por el mismo. Es por esto que el enfoque a través del cual se desarrolla el presente control, se diferencia de los utilizados anteriormente.

Brindar un Prototipo funcional de software, permitirá a la institución tener conocimiento de una solución para satisfacer los requerimientos del proceso de control “*Gestión de los incidentes de la seguridad de la información*”. Además, brinda una herramienta a través de la cual es posible evaluar la solución. También ayuda a clarificar los requerimientos necesarios de la solución y colabora en la identificación de soluciones alternativas.

*“Objetivo del control: Garantizar que los eventos de seguridad de la información y las debilidades asociadas a los sistemas de información se comuniquen de forma tal que se apliquen las acciones correctivas en el tiempo correcto.*

*Se recomienda que se establezcan procedimientos formales de intensificación y reporte de eventos. Es conveniente que todos los empleados, contratistas y usuarios de terceras partes tengan conciencia de los procedimientos para el reporte de los diferentes tipos de eventos y debilidades que podrían tener impacto en la seguridad de los activos de la organización. Se*  
Yustman, Mauricio Ezequiel

*recomienda que ellos reporten cualquier evento o debilidad de seguridad de la información, tan pronto como sea posible, al punto de contacto designado.*

*Objetivo del control: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información.*

*Se recomienda que se establezcan las responsabilidades y procedimientos para manejar efectivamente los eventos y las debilidades de seguridad de la información una vez que hayan sido reportados. Es conveniente que se aplique un proceso de mejora continua para la respuesta, seguimiento, evaluación, y gestión general de los incidentes de seguridad de la información.*

*Cuando se requiera evidencia, se recomienda reunirlos para garantizar el cumplimiento con los requerimientos legales.”*

A continuación, se detallan las pautas/lineamientos a seguir, expuestas por el presente control:

- Establecer un punto de contacto/medio, que sea conocido a través de la organización, que sea de fácil acceso y esté siempre disponible para reportar cualquier evento de seguridad.
- Es conveniente que se establezca un procedimiento formal de reporte de eventos de seguridad de la información.
- Establecer un procedimiento de respuesta a incidente, especificando las acciones a realizar.
- Establecer procedimientos de retroalimentación para garantizar que las personas que reportan los eventos son debidamente notificadas sobre la solución/finalización del mismo.
- Establecer formularios de reporte de eventos de seguridad para dar soporte a esta acción y facilitar la tarea a las personas que realizan esto.
- Se recomienda que la información obtenida a través de los reportes de eventos de seguridad sea utilizada para realizar estudios/mediciones dentro de la organización.

#### 4.9.1 Análisis de la situación actual.

Con el fin de determinar la forma mediante la cual son reportados los eventos de seguridad dentro de la organización, se procedió a realizar una entrevista al jefe del sector de sistemas informáticos y se interrogó al mismo sobre esta temática, teniendo como base los puntos establecidos previamente.

Se determinó que actualmente dentro de la institución los eventos de seguridad de la información son reportados de manera informal (son reportados de manera directa al sector de Sistemas Informáticos). A continuación, se detallan los aspectos más relevantes del caso:

- Cuando los eventos son reportados, los usuarios solamente brindan información muy superficial.
- No se lleva un registro de los eventos reportados ni tampoco las personas que fueron responsable de solucionar los mismos.
- Los eventos de seguridad de la información no están categorizados/tipificados.
- El personal de la institución no está adecuadamente capacitado para poder identificar y detectar un posible evento o debilidad de seguridad de la información, razón por la cual en muchas ocasiones estos no son reportados.

#### 4.9.2 Prototipo.

Se procedió a desarrollar una solución informática que brinde una herramienta para realizar una adecuada gestión de incidentes. Para esto se desarrolló un prototipo funcional denominado “*sistema de gestión de incidentes de seguridad de la información*” (a partir de ahora SGII). Dicho prototipo permite:

- A. Reportar incidentes de seguridad de la información: el sistema brinda una herramienta de fácil acceso para todo el personal de la institución mediante la cual los incidentes de seguridad sean debidamente reportados. La herramienta en cuestión trabaja en un ambiente web que permite al usuario acceder a la misma de manera rápida a través de cualquier navegador. Además, ayuda al usuario a reportar los incidentes respetando el formato establecido.
- B. Gestionar incidentes: el sistema permite al administrador gestionar todos los incidentes reportados por los usuarios. A través de esta herramienta el administrador es capaz de categorizar/sub-categorizar los incidentes de acuerdo a la información brindada por el usuario, asignar un responsable para solucionar/tratar el incidente y realizar un seguimiento del estado de todos los incidentes reportados.
- C. Gestionar tareas a realizar: El sistema brinda al administrador una herramienta mediante la cual establecer una serie de tareas que deben ser realizadas para solucionar/tratar un determinado incidente. A través de esta herramienta el administrador es capaz de establecer tareas por cada subcategoría de incidente, así como también, modificar las mismas o eliminarlas. Esto permite una mayor flexibilidad para establecer los pasos a seguir para tratar los diferentes incidentes de seguridad.
- D. Solucionar/tratar incidentes de seguridad de la información: el sistema permite al responsable asignado para tratar el incidente, conocer las tareas que son necesarias realizar para que este sea debidamente tratado y corregido.
- E. Retroalimentación: El sistema brinda retroalimentación al usuario, permitiendo al mismo, conocer el estado del evento reportado.
- F. Análisis de datos: El sistema permite realizar un análisis de todos los datos recabados por el mismo. Esto ayuda en la toma de decisiones de la alta dirección del hospital
- G. Acceder a documentación referente a la seguridad de la información dentro de la institución: El sistema brinda una herramienta mediante la cual es posible poner a disposición del usuario documentación referente a la seguridad de la información.

#### Herramientas de desarrollo

Para el desarrollo del prototipo (SGII) se utilizaron diferentes herramientas de UML para facilitar así las tareas de diseño y desarrollo del sistema. La documentación elaborada para el diseño del mismo puede ser consultada en el anexo del presente proyecto de grado (ver anexo “SGII”).

En cuanto al lenguaje utilizado y las librerías empleadas para el desarrollo del prototipo, encontramos:

- Lenguaje de Programación: Ruby 2.3.1
- Framework de trabajo: Ruby on Rails
- 4.4.2
- Entorno de desarrollo: Web

Para realizar el desarrollo del prototipo, se empleó una máquina virtual con las siguientes características:

- Procesador de 2 núcleos
- Memoria RAM: 4gb
- Disco Duro: 80gb
- SO: Ubuntu 16.04

Finalmente, se empleó la metodología “Proceso Unificado de Desarrollo de Software”, para la elaboración del prototipo.

#### Acceso a las funcionalidades del prototipo

Para facilitar la evaluación del prototipo desarrollado en el presente proyecto de grado, es posible acceder al mismo a través del siguiente link:  
[https://sgii.herokuapp.com/users/sign\\_in](https://sgii.herokuapp.com/users/sign_in)

A continuación, se indican las credenciales para acceder al sistema:

- Responsable de Seguridad
  - Usuario: adminprueba
  - Contraseña: adminprueba.sgii
- Analista
  - Usuario: analista1.sgii
  - Contraseña: analista1.sgii
- Administrativo
  - Usuario: administrativo1.sgii
  - Contraseña: administrativo1.sgii

Por otro lado, se proporcionan las credenciales de acceso para los correos electrónicos del Responsable de Seguridad y el Administrativo:

- Responsable de Seguridad
  - Correo electrónico: [sgii.adm@gmail.com](mailto:sgii.adm@gmail.com)
  - Contraseña: sgii.adm2016
- Administrativo
  - Correo electrónico: [personal1.sgii@gmail.com](mailto:personal1.sgii@gmail.com)
  - Contraseña: personal1.sgii2016

Se recomienda que, al momento de evaluar el sistema, se emplee el navegador “Google Chrome” para realizar dicha tarea.

También es posible visualizar el funcionamiento general del Prototipo en el inciso **7.10.6** del anexo del presente proyecto

Finalmente, el código fuente del prototipo desarrollado se encuentra adjunto en el CD entregado.

#### 4.9.3 Consideraciones para una adecuada gestión de incidentes de seguridad de la información

Además de la solución propuesta a través del prototipo, deben considerarse los siguientes aspectos para realizar una adecuada gestión de incidentes de seguridad de la información:

- Se debe hacer conocer en toda la organización que este es el medio disponible para el reporte de incidentes de seguridad de la información.
- Los usuarios deben ser capacitados de manera tal que los mismos sean capaces de identificar correctamente cualquier sospecha de debilidad de seguridad de la información y reportar la misma inmediatamente. Para esta capacitación es recomendable elaborar un documento en el cual se detallen los siguientes aspectos:
  - Ejemplificar todos los incidentes categorizados, de manera tal que el usuario sea capaz de identificar fácilmente los mismos y reportarlos
  - Se debe detallar claramente el accionar del usuario en caso de identificar una debilidad de seguridad de la información. Por ejemplo tomar nota de todos los detalles importantes (tipo de mal funcionamiento, mensajes en pantalla, incumplimiento observado), añadir capturas de pantalla/imágenes cuando sea necesario.
  - Aclarar las sanciones previstas en caso de un mal uso del sistema.
- Los usuarios no deben probar o intentar solucionar un incidente/debilidad de seguridad de la información bajo ningún tipo de circunstancia, ya que esto podría ser considerado como mal uso del sistema y conllevar a sanciones para el usuario.
- El SGII permite a los usuarios acceder a información relacionada a la seguridad de la información (acuerdo de confidencialidad, normativas de uso de los recursos informáticos, política de seguridad, leyes aplicables, etc.), por lo tanto se debe prestar especial atención a los permisos de acceso a dichos documentos.

#### 4.9.4 WBS (Estructura de desglose de trabajo)

Se procede a detallar el trabajo realizado para la elaboración del prototipo.

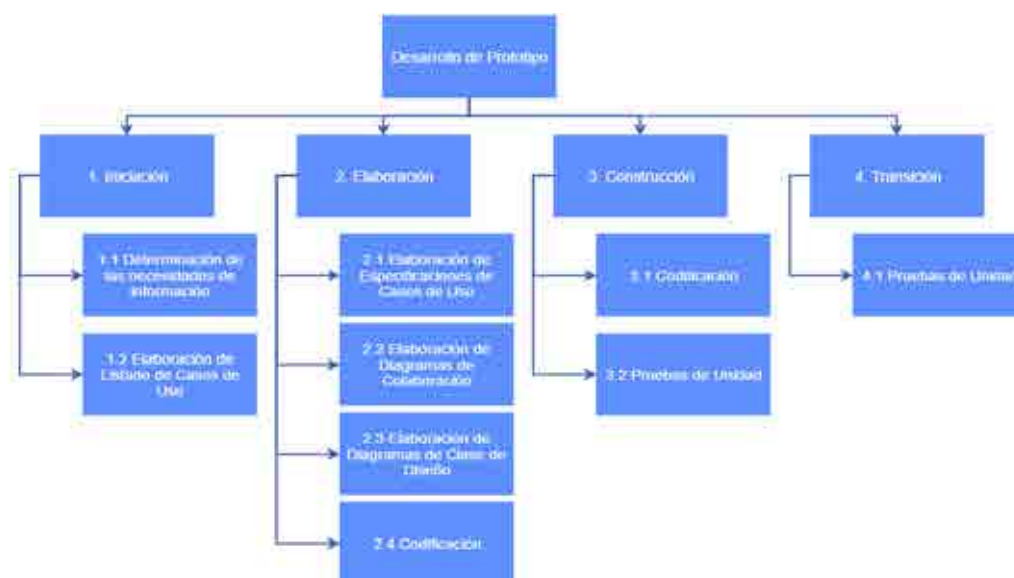


Ilustración 4.9-1

## **Desarrollo del Prototipo**

### **1. Iniciación**

1. Determinación de las necesidades de información: se determinara cual es la información que el sistema debe almacenar y proveer a los usuarios del mismo.
2. Elaboración de Listado de Casos de Uso: Se procede a elaborar el listado de Casos de Uso, que reflejan todas las funcionalidades que debe contemplar el sistema

### **2. Elaboración**

1. Elaboración de Especificaciones de Casos de Uso: se elaboran las especificaciones para cada uno de los casos definidos en el listado mencionado previamente. Se incluye la elaboración del diagrama de clases conceptuales
2. Elaboración de Diagramas de Colaboración: Se generan los diagramas de colaboración, con el propósito de describir el comportamiento dinámico del sistema
3. Elaboración de Diagramas de Clase de Diseño: Se elabora el diagrama de clases
4. Codificación: se procede a traducir en un lenguaje de programación todas las funcionalidades diseñadas en la etapa previa. Durante esta etapa, se procede a preparar el entorno de desarrollo, y se inicia la codificación de las funcionalidades definidas en los primeros casos de uso desarrollados.

### **3. Construcción**

1. Codificación: se procede a codificar las funcionalidades pendientes, conforme a lo definido en la documentación de diseño elaborada.
2. Pruebas de Unidad: se realizarán pruebas para validar el correcto funcionamiento de las funcionalidades elaboradas.

### **4. Transición**

1. Pruebas de Unidad: se procede a realizar pruebas para validar el correcto funcionamiento de todas las funcionalidades del sistema.

#### 4.9.5 Cronograma de actividades

A continuación, se detalla el cronograma de actividades realizadas para la elaboración del prototipo funcional de software

|    | Nombre                                          | Duración | Predecesoras | Recursos                                 |
|----|-------------------------------------------------|----------|--------------|------------------------------------------|
| 1  | ☐ Desarrollo de Prototipo                       | 35.5d    |              |                                          |
| 2  | Inicio de Tareas                                | 0h       |              |                                          |
| 3  | ☐ Iniciación                                    | 2.5d     |              |                                          |
| 4  | Determinación de las necesidades de información | 16h      | 2            | Analista Funcional                       |
| 5  | Elaboración de Listado de Casos de Uso          | 4h       | 4            | Analista Funcional                       |
| 6  | ☐ Elaboración                                   | 13d      |              |                                          |
| 7  | Elaboración de Especificaciones de Casos de Uso | 24h      | 5            | Analista Funcional                       |
| 8  | Elaboración de Diagramas de Colaboración        | 40h      | 7            | Analista Funcional                       |
| 9  | Elaboración de Diagramas de Clase de Diseño     | 8h       | 8            | Analista Funcional                       |
| 10 | Codificación                                    | 40h      | 8            | Analista Programador                     |
| 11 | ☐ Construcción                                  | 15d      |              |                                          |
| 12 | Codificación                                    | 120h     | 9,10         | Analista Programador                     |
| 13 | Pruebas de Unidad                               | 8h       | 10           | Analista Funcional                       |
| 14 | ☐ Transición                                    | 5d       |              |                                          |
| 15 | Pruebas de Unidad                               | 40h      | 12,13        | Analista Funcional, Analista Programador |
| 16 | Fin de Tareas                                   | 0h       | 15           |                                          |

Ilustración 4.9-2

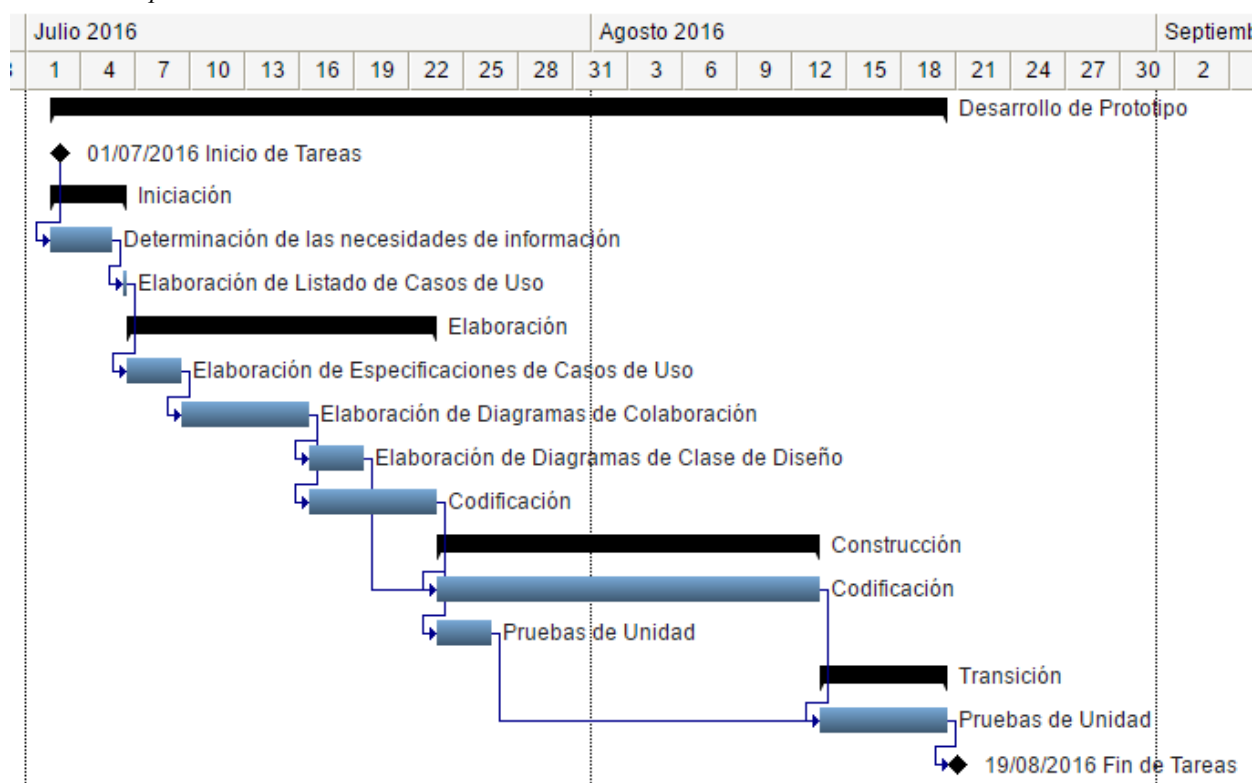


Ilustración 4.9-3

#### 4.9.6 Costos

Considerando que, en el presente control se procedió al desarrollo de un prototipo funcional que coopere en la gestión de los incidentes de seguridad, los costos relacionados en dicho desarrollo son nulos debido a que, al ser un prototipo, no está destinado a ser implementado, sino que su propósito es brindar un modelo de software que ayude a los interesados conocer y probar la solución propuesta.

## 5 Conclusiones y Futuras Líneas de Investigación.

En la actualidad, la información se ha convertido en uno de los activos más importantes (sino, el más importante) para cualquier organización, ya que, a través del tratamiento y procesamiento de la misma, es posible tomar decisiones más acertadas, conocer el estado actual de nuestra organización, realizar proyecciones a futuro, o generar nuevos conocimientos que nos permitan alcanzar una ventaja por sobre los competidores de nuestra empresa, entre otras cosas. Por lo tanto, mantener la confidencialidad, disponibilidad e integridad de la información manejada se ha transformado en una necesidad para las empresas y organizaciones del mundo moderno, y el Hospital Dr. Arturo Oñativia, sobre el cual se ha realizado el análisis de los procesos de seguridad, no es la excepción.

Cabe destacar, además, que la institución bajo estudio posee el deber adicional de mantener la confidencialidad de la información manejada, debido a que la misma es susceptible de generar algún tipo de discriminación a los pacientes que concurren a la misma, en caso de ser divulgada.

Mediante el presente proyecto, fue posible analizar la situación actual, siguiendo los lineamientos establecidos en la Norma IRAM-ISO/IEC 27002:2008, y proponer soluciones realistas, acordes al tamaño de la organización, así como también, realizar la planificación de todas las actividades que el personal de dicho Hospital debe realizar, para la implementación de las soluciones.

Por otra parte, para cada uno de los controles de seguridad desarrollados, se realizó una evaluación de los riesgos a los que se encuentra sujeta la Organización, y de las posibles pérdidas, expresadas en valores monetarios, que la misma podría encontrarse sufriendo al no cumplimentar de manera adecuada con los lineamientos propuestos por la Norma IRAM-ISO/IEC 27002:2008. A través de este análisis, se pretende reflejar la importancia de la Seguridad de la Información dentro del Hospital en términos cuantificables.

Finalmente, cabe destacar que, a pesar de no haberse realizado el análisis de todos los controles de seguridad definidos por la Norma IRAM-ISO/IEC 27002:2008, las soluciones propuestas para los controles evaluados suponen un puntapié inicial para la Organización en cuanto a la gestión de la Seguridad de la Información, de manera que la misma, en el futuro, logre alcanzar una mejora continua de sus procesos de seguridad, permitiéndole adaptarse y responder de manera eficiente a las nuevas amenazas a la seguridad de la información que puedan surgir.

En cuanto a las futuras líneas de investigación, encontramos el análisis y la determinación de soluciones adecuadas para los controles que no fueron desarrollados en el presente proyecto, entre los cuales encontramos:

- Protección Física y Ambiental
- Gestión de la continuidad del Negocio
- Cumplimiento

## 6 Bibliografía

- Norma IRAM-ISO/IEC 27002:2008.
- Sistemas de Información Gerencial (2012). Editorial: Pearson. Autores: Kenneth C. Laudon, Jane P. Laudon.
- Seguridad de la información (2008). Editorial: PARANINFO. Autor: Javier Areitio.
- Técnicas de seguridad informática con software libre (2013). Parque tecnológico de Mérida. Autor: Alejandra Stolk.
- <http://www.segu-info.com.ar/articulos/73-familia-iso-27000.htm>
- [http://www.bajacalifornia.gob.mx/registrocivilbc/iso\\_informa2.htm](http://www.bajacalifornia.gob.mx/registrocivilbc/iso_informa2.htm)
- <http://firmadigital.gba.gov.ar/>
- ¿Cómo funciona la firma digital?  
([https://www.csuc.cat/sites/default/files/docs/como\\_funciona\\_la\\_certificacion\\_digital\\_logonou.pdf](https://www.csuc.cat/sites/default/files/docs/como_funciona_la_certificacion_digital_logonou.pdf))
- <http://latam.kaspersky.com/mx/internet-security-center/definitions/utm>
- <http://segurosyriesgos.com.ar/ calcular-indemnizacion-con-formulas-vuotto-y-mendez/>
- <http://www.welivesecurity.com/la-es/2014/07/01/calculando-perdidas-monetarias-riesgos-seguridad/>
- <https://01seguridad.wordpress.com/2013/09/03/evaluacion-del-riesgo-en-la-informatica/>
- [http://www.shopmcafee.com.ar/store/mfesmb/es\\_MX/pd/productID.306911700/categoryID.66300400](http://www.shopmcafee.com.ar/store/mfesmb/es_MX/pd/productID.306911700/categoryID.66300400)
- <http://www.copaipa.org.ar/>

## 7 Anexo

### 7.1 Normativa de Regulación sobre el Uso de los Recursos Informáticos

#### Regulación Sobre el Uso de los Recursos Informáticos

##### Hospital Dr. Arturo Oñativia

#### Exposición de motivos

El Hospital Dr. Arturo Oñativia proporciona recursos informáticos y servicios de red para su utilización en actividades de investigación, desarrollo, innovación, incluyendo las tareas administrativas asociadas.

Dado que estos recursos y servicios son ampliamente utilizados y que la red sobre la que están soportados será integrada a su vez en otras de índole más amplia, se hace necesaria la aprobación de una normativa que clarifique la forma correcta de uso de los mismos, delimite las responsabilidades y proporcione un marco para la regulación del uso de cada uno de ellos.

#### Objeto de la normativa

La presente normativa tiene por objeto la regulación del uso de los recursos informáticos y servicios de red que el Hospital Dr. Arturo Oñativia proporciona para su utilización en actividades de investigación, desarrollo e innovación y tareas administrativas.

#### Principios rectores

Los principios generales en que se inspira esta regulación son los siguientes:

- Proteger el buen nombre y el prestigio del Hospital Dr Arturo Oñativia, así como de los Centros, Departamentos, Áreas, Sectores y Servicios que lo constituyen.
- Evitar situaciones que puedan causar al Hospital Dr Arturo Oñativia algún tipo de responsabilidad civil, administrativa o penal.
- Facilitar el máximo aprovechamiento de los medios informáticos, propiciando una gestión eficiente de los procesos incluidos en sus sistemas de información y redes de comunicaciones con las que opera.
- Prevenir los riesgos o daños sobre los sistemas de información y los datos en ellos incorporados que puedan deberse a la acción humana, referente a conductas incorrectas o inadecuadas.

#### Definiciones

A los efectos de la presente normativa se entenderá por:

- Recursos informáticos: Todos los medios de cualquier naturaleza, físicos o lógicos que intervienen en los sistemas de información y en las redes de comunicaciones.
- Red de Comunicaciones hospitalaria: Infraestructura de comunicaciones de propiedad o bajo la supervisión del Hospital Dr Arturo Oñativia accesible por todos los empleados y trabajadores del hospital mediante la cual se transmiten las comunicaciones de datos, imágenes y señales de control. Esta red (intranet hospitalaria) para permitir la comunicación completa está conectada con redes externas que constituyen lo que se denomina extranet.
- Servicio de red: Cualquier servicio o aplicación que utiliza la red hospitalaria y que permite a los usuarios comunicarse entre sí o con terceros y acceder o compartir

información, a través la intranet o a la extranet. Son ejemplos de servicios de red: el correo electrónico, servidores de páginas web, internet, etc.

- Usuario: Es la persona que tiene alguna vinculación con el Hospital y utiliza los recursos o servicios informáticos ofrecidos por el mismo.
- Contraseña: Información, frecuentemente constituida por una cadena de caracteres, que se utiliza en el proceso de autenticación de un usuario.
- Identificación y autenticación: Procedimientos de reconocimiento y comprobación, respectivamente, de la identidad de un usuario.
- Control de acceso: Mecanismo que en función a la identificación y autenticación permite acceder a un espacio virtual restringido.
- Espacio virtual restringido: Conjunto de procesos e información cuyo acceso está restringido a un conjunto de personas. La entrada a dicho acceso se limita por un sistema de control de acceso.
- Cuenta de usuario: Se denomina así a la personalización de un servicio de red para su uso por un usuario. Normalmente la utilización personalizada de un servicio de red conlleva la asignación de un identificador y una contraseña los cuales deben ser de uso exclusivo de la persona debiendo ser estos resguardados celosamente, los cuales permiten al usuario la utilización personal de dicho servicio y el acceso al espacio virtual restringido del mismo. Por ejemplo, la cuenta de usuario del correo electrónico.
- Servidor: Equipo informático que proporciona a los usuarios uno o varios servicios de red. (por ejemplo, un servidor de archivos o un servidor de correo electrónico)
- Lista de distribución: Servicio de red que agrupa a un conjunto de direcciones electrónicas bajo un solo nombre “lista” y permite enviar mensajes de correo electrónico a todas las direcciones incluidas en la lista.

### **Ámbito de aplicación**

La presente regulación es aplicable a todos los miembros de la comunidad hospitalaria, tanto a nivel individual como colectivo (áreas, sectores, servicios, etc.) en cuanto que hagan uso de recursos informáticos o servicios de red, así como a cualquier otra persona o entidad externa al Hospital que los utilice.

Con objeto de dar la mayor publicidad a esta normativa, el Sector de Informática del Hospital dispondrá de los medios necesarios para permitir su consulta de forma fácil, teniendo en cuenta que el desconocimiento de esta normativa no exime de su cumplimiento.

### **Criterios de utilización de los recursos informáticos y los servicios de red**

La utilización de los recursos informáticos y servicios de red del Hospital Dr. Arturo Oñativia se ajustará a las previsiones generales en materia de protección de datos de carácter personal, propiedad intelectual y protección del honor e intimidad y, en su caso, a las propias de este Hospital. De manera específica, la utilización de los citados recursos se ajustará a los siguientes criterios:

- En ningún caso, se podrán utilizar los recursos informáticos del Hospital Dr. Arturo Oñativia para actividades que sean contrarias al ordenamiento jurídico. De modo particular queda prohibido difundir contenidos de carácter discriminatorio de cualquier tipo, pornografía infantil o de cualquier otro tipo, sexista, de apología del terrorismo, de incitación a la violencia o atentatorio contra los derechos humanos, así como actuar en perjuicio de los derechos a la intimidad, al honor, a la propia imagen, contra la dignidad de las personas o contra la protección de datos de carácter personal.

- Los medios indicados están destinados al uso profesional de los usuarios, por tanto, éstos no disponen del uso privativo de los mismos.
- Los usuarios destinarán los medios indicados a usos compatibles con la finalidad de las funciones del servicio al que se encuentren adscriptos y que correspondan con su trabajo. Su utilización con cualquier otro fin diferente necesitará del consentimiento expreso de la autoridad competente en el Hospital.
- Los usuarios deberán realizar un adecuado uso y cuidado de los medios materiales puestos a su disposición.
- Queda prohibida cualquier tipo de publicidad no contratada por el Hospital Dr. Arturo Oñativia, así como la información privilegiada a favor del propio autor o familiares.
- Queda prohibido el uso de programas o actividades que hagan uso abusivo del tráfico de red, ya que esto entorpecería el correcto y eficiente funcionamiento de los sistemas informáticos destinados al trabajo cotidiano del Hospital; ejemplo de esto son:
  - El uso de programas de compartición de archivos (file sharing), como Ares, Kazaa, e-mule, e-donkey, torrent, entre otros, para la descarga de películas, mp3, etc.
  - Programas de mensajería o chat, como Messenger, Yahoo Chat, Google Talk, ICQ, etc., para mantener conversaciones personales y ajenas a las tareas que se desarrollan dentro del Hospital.
  - El uso de sitios del tipo streaming, tales como radios, televisión, cine o música online.
  - Todo tipo sitios de reproducción de videos o películas online como por ejemplo YouTube, megavideo, etc.
  - Juegos online.
  - Etc.
- La instalación de nuevo software en las estaciones de trabajo deberá ser realizada exclusivamente por personal perteneciente al sector Informática del Hospital o bajo el consentimiento del mismo.
- Queda prohibido el uso de software que viole las leyes respecto a la propiedad intelectual, esto incluye software ilegal o pirata. En la actualidad aproximadamente el 90% del software instalado en las maquinas tiene este carácter, progresivamente se irá revirtiendo esta situación reemplazando el soft mencionado con software legamente soportado, quedando prohibido el uso de nuevo soft que no cumpla con las leyes antes mencionadas.

### **Incumplimiento de las Condiciones de Uso**

- Se considera incumplimiento de las Condiciones de Uso cualquier actuación que no se ajuste a las previsiones establecidas en la presente normativa. Especialmente, los supuestos siguientes:
- La sustracción o el traslado no debidamente autorizado a otras dependencias, de cualquier elemento físico de la instalación informática o de la infraestructura complementaria, así como el causar daños a los mismos.
- La búsqueda o utilización de identificadores y contraseñas de otros usuarios o cualquier intento de encontrar y explotar fallos en la seguridad de los sistemas informáticos del Hospital o de fuera, o hacer uso de aquellos sistemas para atacar cualquier sistema informático.
- El acceso a cualquier espacio virtual restringido para el que no se dispone de la debida autorización.
- Los usos ilícitos por parte de terceras personas de cuentas de usuarios

- (usuario/contraseña) en los sistemas informáticos (con conocimiento de los usuarios oficiales), tanto por quien realiza el acceso indebido como por el responsable de la cuenta, así como, el incumplimiento de los términos de licencias del software genérico adquirido en el Hospital.
- La introducción intencionada de virus, “caballos de Troya”, “gusanos”, “bombas de tiempo” o cualquier otro software perjudicial o nocivo.
  - La no confidencialidad de los datos a los que, bien como parte de su trabajo o bien por accidente, se haya accedido.
  - Saboteo del uso de la red mediante la congestión de enlaces o sistemas informáticos, interceptación de las comunicaciones y la utilización de técnicas de escucha, transmisión, grabación o reproducción de cualquier señal de comunicaciones.
  - La alteración de la integridad, uso o manipulación indebida de los datos.
  - El uso indebido de los servicios de Red, para comunicarse con otros usuarios, cuando causen:
    - Actividades ilícitas o ilegales de cualquier tipo y particularmente, difundir contenidos o propaganda de carácter racista, xenófobo, pornográfica, sexista, de apología del terrorismo o atentatorio contra los derechos humanos o actuar en perjuicio de los derechos a la intimidad, al honor, a la propia imagen o contra la dignidad de las personas.
    - Difusión de contenidos atentatorios contra los principios rectores del Hospital.
    - Suplantaciones de direcciones de la red.
    - Recopilación de información sobre terceros de carácter personal sin su consentimiento.
    - Creación de identidades falsas con el fin de engañar a terceros respecto de la identidad del remitente o del origen de la comunicación.
    - Utilizar los medios de la red con fines propagandísticos y comerciales, sin autorización expresa.
    - Difusión de manifestaciones o referencias falsas, incorrectas o inexactas sobre las páginas y servicios del Hospital.
    - No mantener los recursos informáticos bajo su responsabilidad con las medidas de seguridad necesarias.
  - Instalación de software en los equipos o realización de configuraciones especiales en los mismos sin el consentimiento del personal perteneciente al Sector Informática del Hospital Dr. Arturo Oñativia.

### **Responsables del incumplimiento**

Serán responsables del incumplimiento de la normativa los usuarios que realicen las conductas tipificadas como malas o incorrectas en esta normativa y, en su caso, los responsables de los recursos correspondientes, en caso de existir dolo o negligencia grave, previa tramitación del correspondiente procedimiento.

Cada usuario es responsable por el correcto y adecuado uso de los recursos informáticos que se le asignan.

El Hospital Dr. Arturo Oñativia como así también el Sector responsable de la administración y gestión de los Sistemas Informáticos pertenecientes al mismo, no se responsabilizará por los daños o perjuicios producidos a terceros por el uso indebido de los recursos informáticos, siendo responsabilidad directa y exclusiva del usuario que incumple con dolo o negligencia grave las normativas presentadas en esta reglamentación.

### **Actuaciones en caso de incumplimiento**

En caso de incumplimiento de la presente regulación, se advertirá del hecho al infractor, pudiéndose acordar con parte a la Gerencia del Hospital la suspensión temporal con carácter cautelar del acceso a los recursos informáticos y servicios de red. En caso de que el usuario no responda o ignore la advertencia, se podrán adoptar, previa la tramitación del correspondiente procedimiento, las disposiciones pertinentes para proceder a una suspensión total del acceso a tales recursos y servicios.

Todo lo anterior se entiende sin perjuicio de las acciones disciplinarias, administrativas, civiles o penales que en su caso correspondan, a las personas implicadas en dicho incumplimiento.

Además, el Hospital se reserva el derecho a iniciar, en su caso, las acciones oportunas en aquellos casos que, si bien no están directamente previstos en la presente normativa, si pueden estar contemplados en el código penal o en cualquier otra normativa vigente, especialmente, en materia de protección de datos de carácter personal o de propiedad intelectual o industrial.

### **Disposiciones finales**

El Sector de Informática del Hospital Dr. Arturo Oñativia queda habilitado para desarrollar lo señalado en esta normativa, aprobada por la Gerencia del Hospital, estableciendo Condiciones de Uso específicas para aquellos recursos o servicios que se considere necesario. De lo cual dará cuenta a la misma y formando parte, como anexo de esta normativa.

La presente regulación entrará en vigor a partir del día 21/09/2010.

## 7.2 Contexto Organizacional

A continuación, se presenta el organigrama completo del hospital:

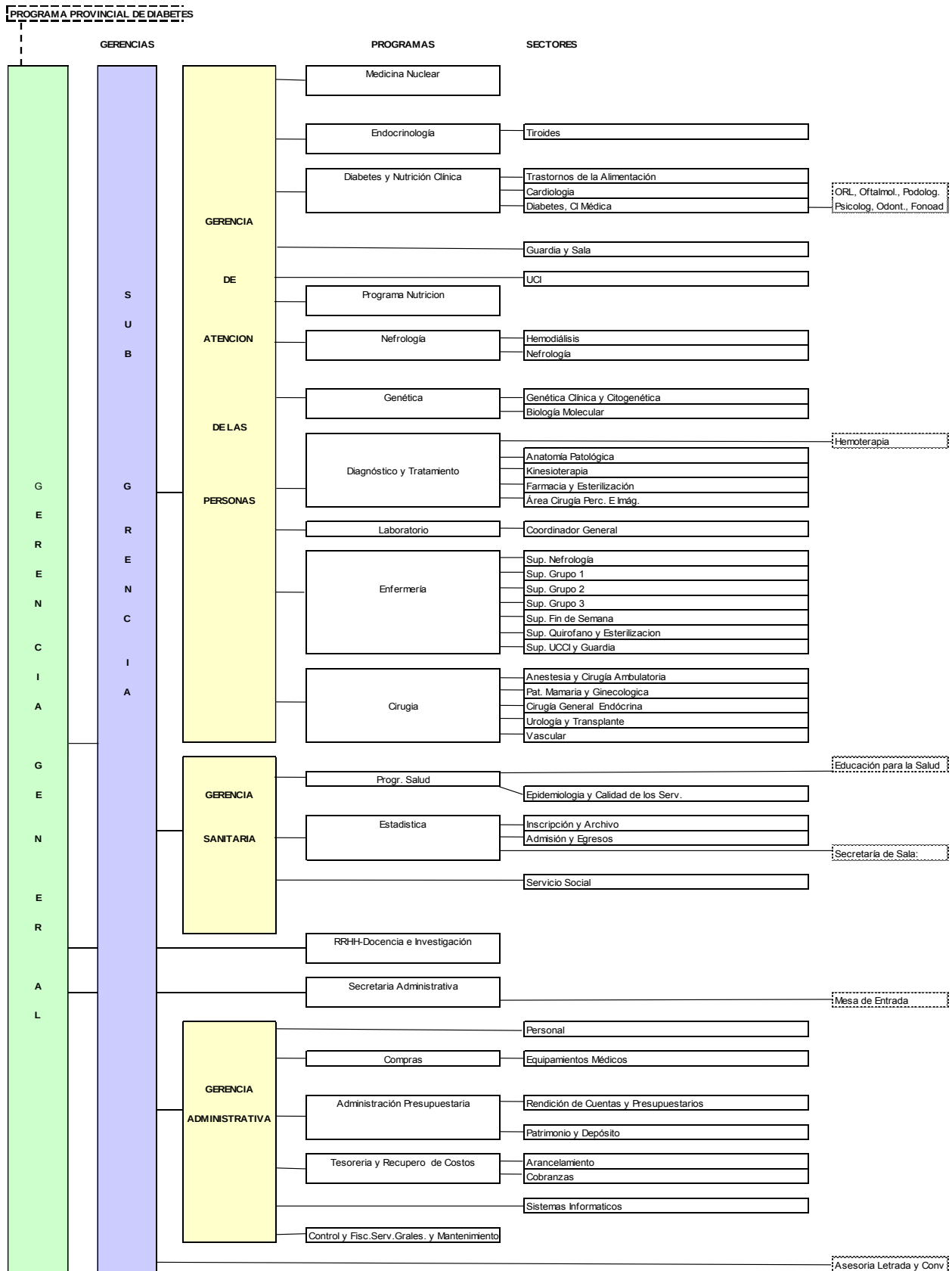


Ilustración 7.2-1

A continuación, se presenta un organigrama que incluye únicamente las áreas bajo estudio junto con sus respectivas misiones y funciones

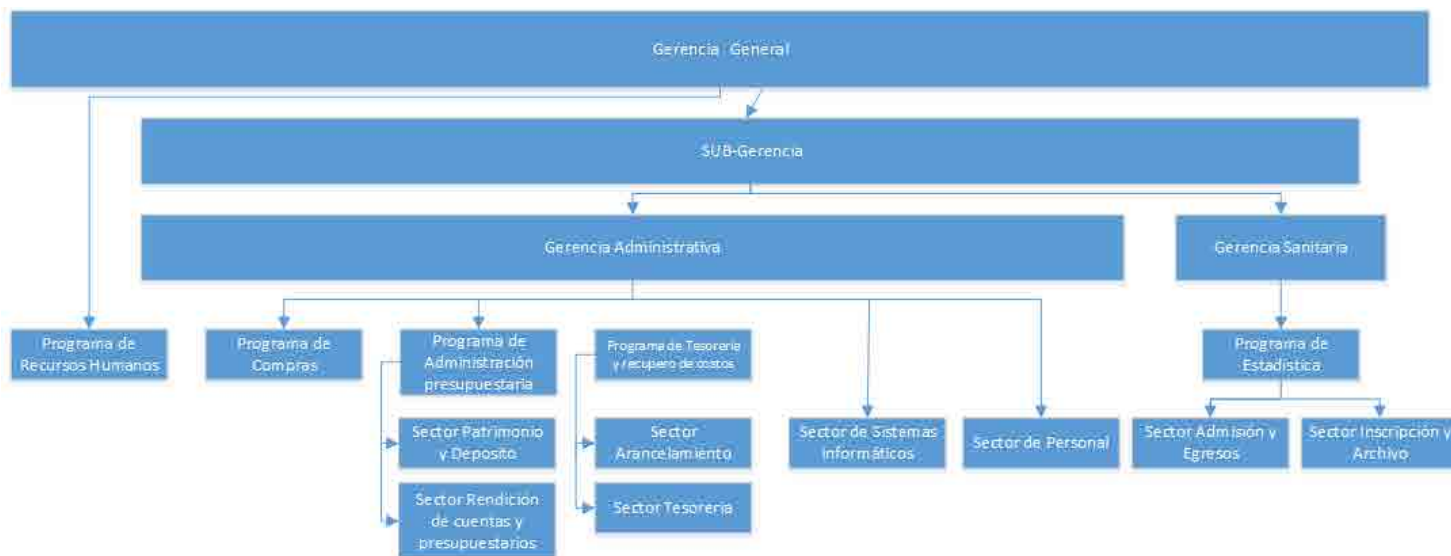


Ilustración 7.2-2

Con el propósito de explicar la labor realizada por cada sector/programa, se detalla la misión y función de cada uno de ellos (Información obtenida a través del relevamiento realizado en la institución. Documentación que contiene la misión, visión y función de cada sector/programa del hospital). A continuación, se detallan los aspectos más relevantes de cada sector.

### **Gerencia General**

#### *Misión:*

Gestionar de manera integral los servicios brindados por el hospital con el propósito de brindar un servicio de calidad para el paciente. Gestionar, planificar, controlar y corregir todas las actividades relacionadas a los servicios brindados por el hospital.

#### *Funciones:*

- Gestionar integralmente el hospital.
- Toma de decisiones que hacen a la resolución de problemas y temáticas hospitalarias
- Determinar las metas organizacionales.
- Supervisar las actividades desarrolladas en el hospital.
- Determinación y Organización de los servicios brindados por el hospital.
- Coordinar y gestionar los proyectos institucionales.
- Dirigir y controlar las actividades.
- Administrar el presupuesto general de la institución.

### **Programa de recursos humanos**

#### *Misiones:*

Atender en lo relativo a la Administración local de Recursos Humanos de los agrupamientos Profesional, Enfermería, Técnico y Administrativo y coordinación con los pertenecientes a Servicios tercerizados, en todos los campos de importancia decisiva para el funcionamiento eficiente de los servicios de salud que allí se prestan.

*Funciones:*

- Ejecutar los planes y programas de capacitación que hayan sido aprobados.
- Propiciar la constitución y el sostenimiento de los Comités Hospitalarios.
- Mantener actualizados en la Institución los Legajos y Control de Cargos a través del Sector Personal.
- Asesorar a nivel Gerencial de la Institución en relación a la determinación de los perfiles de cargos y necesidades de cada área a fin de que puedan adecuarse y optimizarse las aptitudes y capacidades de cada agente en relación a la tarea y resultados esperados.
- Estimular a las personas a que sean artífices de su perfeccionamiento con vocación de servicio y responsabilidad, generando incentivos para dicho cometido.
- Fortalecer el desarrollo de la carrera profesional y administrativa por la vía de concursos para cubrir funciones jerárquicas.
- Propiciar mecanismo para el fortalecimiento del clima organizacional adecuado, a través de la motivación y mediación en la relación de conflictos.
- Interactuar con Programas de Recursos Humanos de otros efectores de Salud Pública guardando relación con la Dirección de Recursos Humanos del Nivel Central, para la puesta en común de la Problemática de cada área que permita compartir experiencias e identificar probables soluciones.

**Programa de estadística**

*Misiones:*

Brindar información estadística, epidemiológica y socio-demográfica permanente para la toma de decisiones en la gestión, administración hospitalaria y para las actividades de Docencia e investigación del Hospital. Formar para del sistema Provincial y Nacional de Estadísticas e información de Salud.

*Funciones:*

- Elaborar la planificación de sus áreas con el propósito de alcanzar sus objetivos.
- Coordinar acciones con los demás Jefes de Programas.
- Gestionar la provisión de recursos e insumos necesarios para la tarea diaria.
- Capacitar al personal a su cargo.
- Supervisar los procesos para el logro de los objetivos.
- Elaborar, analizar y difundir los indicadores de producción hospitalarios en forma oportuna para la gestión, investigación y docencia.
- Participar en los comités hospitalarios.
- Cumplimentar con los requerimientos de documentación del área de Medicina Legal.
- Cumplimentar con los requerimientos del nivel provincial y nacional del sistema Estadístico.

- Inducir a la comunidad hospitalaria al manejo y uso de la información que se produce en sus áreas.
- Custodiar la integridad y calidad de las Historias Clínicas según leyes vigentes.
- Custodiar la integridad y calidad de las bases de datos del paciente y los profesionales intervinientes según leyes vigentes.

### **Sector inscripción y archivo**

#### *Misión*

Coordinar y Supervisar los procesos de inscripción de pacientes para la consulta ambulatoria y archivo de documentación generada durante la atención.

#### *Funciones:*

- Supervisar el proceso referente a la inscripción de pacientes ambulatorios.
- Verificar el registro de datos necesarios para la consulta y su calidad de atención, como así también de toda aquella información que permita monitorear los movimientos de Historias Clínicas.
- Reguardar el archivo diario de Historias Clínicas.
- Mantener permanente actualizado la agenda de turnos para la consulta médica.
- Monitorear permanente el procedimiento de atención en el Servicio 0800, coordinando todas las acciones necesarias para la optimización de su funcionamiento.
- Informar a Jefatura de Programa los indicadores producidos en la consulta externa y archivo.

### **Sector admisión y egresos**

#### *Misión.*

Coordinar y Supervisar los procesos de Admisión y Egresos de pacientes.

#### *Funciones:*

- Supervisar los procedimientos de apertura de Historia Clínica de pacientes que requieran internación
- Coordinar las actividades inherentes a Secretaría de Salas,
- Verificar que las Historias Clínicas cumplan con los requisitos necesarios para su procesamiento y archivo.
- Mantener interrelación con otros Programas y/o Sectores.
- Informar a Jefatura de Programa indicadores de Producción y Rendimiento.

### **Programa de Tesorería y recupero de costos.**

#### *Misión*

El programa de Tesorería y recupero de costos tiene como finalidad administrar, registrar y controlar los recursos financieros del Hospital, cumpliendo las obligaciones determinadas en el Presupuesto.

#### *Función:*

*Yustman, Mauricio Ezequiel*

*Pérez Osán, Fernando Javier*

- Recepcionar y mantener en custodia los libramientos ingresados hasta tanto se produzca su pago o su caducidad.
- Cumplir con las Órdenes de Pagos siguiendo los lineamientos establecidos por el Ministerio de Finanzas y Obras Públicas.
- Suministrar a Contaduría General la información necesaria respecto del estado de pago de los libramientos
- Registrar los ingresos y pagos de las Cuentas Bancarias del Tesoro y conciliar sus saldos.

### **Sector Arancelamiento**

#### *Misión:*

Regular la facturación realizada a las obras sociales y demás prestadoras asistenciales por las prácticas que se realizan en el hospital a sus beneficiarios, con el fin de recuperan parte de los gastos médicos derivados de la actividad.

#### *Función:*

- Garantizar la gratuidad del acceso a la atención de la salud, como así también la máxima cobertura posible de acuerdo a nuestro nivel de complejidad a toda la población no cubierta por los restantes subsistemas de atención de la salud.
- La tramitación de toda la documentación necesaria para gestionar el cobro de los servicios brindados al paciente que pertenece a una obra social.
- La facturación de la documentación obtenida para que la misma sea presentada para su posterior cobranza

### **Sector Tesorería**

#### *Misión:*

Administrar y controlar los recursos financieros del hospital. Garantizando que los mismos sean acordes al presupuesto hospitalario.

#### *Función:*

- Recaudar, custodiar y depositar los bienes financieros de la Institución.
- Gestionar el pago a los empleados de la institución.
- Gestionar el pago a terceros.
- Administrar los gastos diarios de caja chica.
- Gestión de los cobros, realizando los ingreso en el/los banco/s de los distintos medios de pago utilizados.
- Remitir al Departamento de Contabilidad, el informe diario de las operaciones bancarias, de dispersión de fondos, ingresos y egresos.

### **Sector personal**

#### Misión

El Sector Personal cuya misión consiste en Coordinar y apoyar toda la Administración de personal, aplicar y hacer cumplir las disposiciones legales y administrativa vigente en materia de personal, este Sector realiza la tarea de:

- Control de Asistencia
- Legajos
- Control de Cargos
- Liquidaciones

Funciones:

- CONTROL DE ASISTENCIA: donde se reflejan las distintas actividades de personal, y de acuerdo a la implementación de los relojes biométricos: se carga los datos con las declaraciones juradas.
- LEGAJOS:
  - Se responsabiliza por el Legajo del Personal de Planta Permanente, Designación Temporaria, Residentes y confecciona los mismos al momento de ingreso.
  - Recibir, controlar, registrar y conservar toda la documentación relativa al Legajo
  - Registrar las tomas de posesión y actualizar por medio del registro la situación del empleado por traslado, afectaciones, asignaciones y/o baja de funciones, modificación del régimen horario, Modificación de agrupamiento, subgrupo, pago de licencias adeudadas a los agentes renunciantes, extinguido relación laboral.
- CONTROL DE CARGOS:
  - Intervenir directamente con los trámites de expedientes relativos a las tramitaciones, designaciones, renuncias, asignaciones de funciones, afectaciones, traslados, modificación de situación de revista.
  - Registro de instrumentos legales, Decretos, Resoluciones Ministeriales, Disposiciones Internas.
- LIQUIDACIONES:
  - Confeccionar las novedades de altas y bajas de haberes del personal.
  - Confeccionar fichas de seguros de vida.
  - Intervenir en todas las actuaciones que se relacionan con embargos.
  - Llevar individual y permanentemente un registro documentados de las situaciones que incidan en la determinación de haberes.

### **Sector informática**

#### **Misión**

Articular, desarrollar y mantener los medios necesarios para gestionar los recursos informáticos, en pos de lograr se conviertan en herramientas útiles para perfeccionar y optimizar los procedimientos de gestión con el apoyo del hardware y/o software necesario. Gestionar y poner a disposición información confiable, logrando un mejor aprovechamiento de la misma, mediante el uso técnicas de análisis y herramientas informáticas, para facilitar el proceso de toma de decisiones en pos de una mejora en la calidad de atención.

#### **Funciones:**

- La función principal está encaminada por el óptimo funcionamiento de los recursos informáticos y los sistemas de información que apoyan a toda la gestión de la institución.
- Generación de protocolos e instructivos sobre el uso de los recursos informáticos.

- Analizar, programar y desarrollar módulos para un sistema integrado que responda a las necesidades de los usuarios.
- Administrar y mantener los sistemas informáticos actualizados.
- Administración de servicios de servidores.
- Velar por la integridad de la información almacenada en equipos servidores de propiedad institucional.
- Elaborar y ejecutar los planes de contingencia
- Mantenimiento: El hospital cuenta con diversos equipos informáticos los cuales se realiza mantenimiento continuo con el propósito de optimizar su rendimiento, prolongar su vida útil y lograr que cumplan su función. Básicamente los equipos a los cuales se realiza mantenimiento son: Computadoras de escritorio, Notebook, impresoras, proyectores, equipos de conectividad.

#### Estructura del sector de sistemas informáticos:

Actualmente, el Sector de Sistemas Informáticos cuenta con un personal constituido por 3 personas, los cuales cumplen con los siguientes roles:

A. Analistas programadores/ funcionales (2 personas): Estos profesionales están dedicados exclusivamente al análisis, mantenimiento, adaptación, corrección y generación de sistemas informáticos. Realizan tareas de:

- Análisis de requerimiento de los usuarios
- Desarrollo de sistemas
- Generación de soluciones para problemas de gestión de la información
- Adaptación/corrección/supervisión de sistemas informáticos.
- Asesoramiento en la contratación de servicios específicos en donde la informática, tecnología o gestión de la información se vean involucradas.
- Capacitación.

B. Técnico de soporte (1 persona): Esta persona posee los conocimientos técnicos adecuados para gestionar y mantener el buen funcionamiento de los equipos que dan soporte a la gestión de la información, tales como computadoras e impresoras. Además, esta persona se encarga de tareas como:

- Gestión de insumos (cartuchos, respuestas, etc.)
- Asesoramiento para la compra de equipamiento.
- Gestión básica de la red LAN. (instalación de nuevas bocas de red)
- Brindar ayuda al usuario en el uso de los recursos informáticos que posee la institución.

#### **Programa de compras**

Misión:

Brindar apoyo en las tareas de compras requerida en la institución. Funcionar de nexo entre el hospital y los proveedores.

Funciones:

*Yustman, Mauricio Ezequiel*

*Pérez Osán, Fernando Javier*

- Manejo de licitaciones y compras directas a proveedores.
- Búsqueda de calidad de los productos requeridos.
- Manejo de las listas de proveedores.
- Búsqueda de proveedores.
- Contacto con proveedores.

### **Programa de administración presupuestaria**

#### *Misión*

Atender el cumplimiento de todas las tareas administrativo-contable vinculada al movimiento financiero, patrimonial, tareas inherentes a las rendiciones de cuentas del hospital, de acuerdo a las normas y disposiciones legales en vigencia.

#### *Funciones:*

- Registrar el movimiento financiero del hospital, conforme a los ingresos provenientes de tesorería general de la provincia, nacional y los recursos propios de arancelamiento.
- Solicitar mediante expediente al Min. De salud pública la cuota mensual para bienes de consumo-servicios y los fondos para el pago de sueldo al personal y refuerzos de crédito del presupuesto
- Realizar órdenes de pagos de sueldos, Litis, embargos, retenciones y proveedores.
- Atención a proveedores, recepción de órdenes de compras y facturas.
- Realizar rendición de arancelamiento proveniente de la recaudación diaria de las prestaciones a particulares y a obras sociales.
- Proveer la documentación solicitada a los distintos organismos auditores.
- Proveer información oportuna y confiable que permita tomar decisiones a los jerárquicos de la institución.

### **Sector Rendición de cuentas y presupuestarios**

#### *Misión*

Efectuar el control de las rendiciones de cuentas de conformidad a las disposiciones legales vigentes.

#### *Funciones:*

- Recepción de toda orden de pago emitida, revisión minuciosa de cada comprobante y controlar que la misma cuente con la imputación de gasto correspondiente.
- Realizar las planillas de rendiciones de cuentas registrando los cargos de valores recibidos y descargos de las órdenes de pago de los gastos realizados.
- Intervenir en la guarda de toda la documentación.

### **Sector patrimonio y deposito**

#### *Misión*

Llevar el control cualitativo y cuantitativo de los bienes patrimoniales

#### *Funciones:*

*Yustman, Mauricio Ezequiel*

*Pérez Osán, Fernando Javier*

- Velar por el cuidado, buen uso y conservación de los bienes muebles del patrimonio del hospital.
- Identificar y marcar los bienes que se incorporan al patrimonio aplicando los clasificadores aprobados según normas vigentes.
- Realizar expedientes por transferencia de bienes, donaciones altas, bajas y sustracciones de bienes.
- Solicitar reparación de bienes.
- Realizar trámites en telefonía por los celulares asignados al personal de la institución.

### 7.3 Acuerdo de confidencialidad

#### ACUERDO DE CONFIDENCIALIDAD

“Entre la .....(Organización), con domicilio en ..... , Código Postal ..... , de la ..... , representada en este acto por ..... , con DNI N° ..... , en adelante “LA INSTITUCION”, por una parte; y por la otra parte, el/la Sr./a , con domicilio en ..... , Provincia de..... , con DNI N° ..... , en adelante “EL EMPLEADO”, quienes en lo sucesivo se denominan en forma conjunta e indistinta LAS PARTES, y declaran:

- a) Que EL EMPLEADO se encuentra contratado por LA FUNDACIÓN para cumplir diferentes funciones o brindar determinados servicios.
- b) Que sin perjuicio de las obligaciones de secreto y reserva previstas en el Art. 85 de la Ley 20.744 y en la Ley 24.766, se considera necesario especificar el más amplio alcance de dichas obligaciones.

#### **CLÁUSULAS**

##### **PRIMERA - Definiciones**

“Información Confidencial” comprende, de manera colectiva, toda la información que sea suministrada por LA INSTITUCION AL EMPLEADO, en el desarrollo de la relación laboral, al igual que todos los datos de índole financiera y/o comercial, conceptos, técnicas, principios y demás conceptos subyacentes a sus sistemas y aplicaciones informáticas a los que pudiera tener acceso como consecuencia del desarrollo de sus funciones, así como otros datos e información, análisis, estudios, notas, recopilaciones, resúmenes, memorandos, informes y conclusiones o cualquier otro documento preparado por LA INSTITUCION (incluyendo sus

*empleados, asesores o representantes) relacionada con las actividades propias LA INSTITUCION.*

*Así mismo se entiende como Información Confidencial: (i) La información que no sea pública y sea conocida por EL EMPLEADO con ocasión del desarrollo de sus funciones, bien sea que la misma sea escrita, oral o visual, (ii) Cualquier tipo de información relacionada con el funcionamiento de LA INSTITUCION, su infraestructura, hardware, software (S.O. Y Software de gestión), datos, usuarios, comunicaciones y seguridad Informática; (iii) Cualquier tipo de información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, modelos de negocios y cualquier otra relacionada con las operaciones de negocios presentes y futuros de LA INSTITUCION, y/o relacionada con su estructura organizacional o de sus clientes, bien sea que la misma sea escrita, oral o visual, o en cualquier forma tangible o no, incluidos los Mensajes de Datos, de la cual EL EMPLEADO tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud del desarrollo de sus funciones.*

#### **CLAUSULA SEGUNDA - Manejo de la información confidencial**

*EL EMPLEADO reconoce de manera expresa, la naturaleza confidencial de toda la Información Confidencial que le suministre y le haya suministrado LA INSTITUCION y el hecho de que es de su propiedad exclusiva. En consecuencia, EL EMPLEADO acepta y está de acuerdo en que:*

- (i) Sólo utilizará la Información Confidencial con el propósito exclusivo de desarrollar las funciones para el cual fue contratado.*
- (ii) No permitirá el acceso a la Información Confidencial ni divulgará de manera parcial o total su contenido a ningún tercero, sin el consentimiento escrito u oral previo de LA INSTITUCION, salvo en los casos en que sea necesario divulgar ese contenido con el propósito exclusivo de que trata el numeral anterior.*

#### **CLAUSULA TERCERA - Información no sujeta a confidencialidad o reserva**

*Sin perjuicio de lo estipulado en el presente Acuerdo, ambas partes aceptan que la obligación de confidencialidad no se aplicará en los siguientes casos:*

- (i) Cuando la información se encontrará en el dominio público en el momento de su suministro al RECEPTOR o, una vez suministrada la información, ésta acceda al dominio público sin infracción de ninguna de las Estipulaciones del presente Acuerdo.*
- (ii) Cuando la información ya estuviera en el conocimiento del RECEPTOR con anterioridad a la firma del presente Acuerdo y sin obligación de guardar confidencialidad.*
- (iii) Que EL EMPLEADO la haya obtenido sin obligarse a guardarla en reserva, de fuente distinta a LA INSTITUCION y sin que dicha fuente esté desconociendo o violando un pacto de reserva o confidencialidad.*
- (iv) Cuando LA INSTITUCION expresamente autorice su divulgación.*

#### **CLAUSULA CUARTA - Obligaciones de la parte receptora.**

*Yustman, Mauricio Ezequiel*

*EL EMPLEADO receptor de la Información Confidencial se obliga a mantener estricta confidencialidad sobre la documentación e información que conozca, reciba o intercambie con ocasión de la relación laboral. En particular, se obliga a:*

- 1. Proteger la confidencialidad de la información verbal, escrita o que por cualquier otro medio reciba de LA INSTITUCION, obligándose en forma irrevocable ante LA INSTITUCION a no revelar, divulgar o facilitar -bajo cualquier forma- a ninguna persona física o jurídica, sea esta pública o privada, y a no utilizar para su propio beneficio o para beneficio de cualquier otra persona física o jurídica, pública o privada, toda la información relacionada con el ejercicio de sus funciones, como así también las políticas y/o cualquier otra información vinculada con sus funciones y/o el giro comercial de LA INSTITUCION.*
- 2. Usar toda la Información Confidencial que se le entregue o que produzca solamente a los efectos del desarrollo de sus funciones. Igualmente, se obliga a mantener dicha información en reserva hasta tanto adquiriera carácter público.*
- 3. Implementar mecanismos adecuados para proteger la confidencialidad de la misma guardando dicha Información Confidencial en un lugar de acceso restringido y con las mismas seguridades que utiliza para su propia información confidencial.*
- 4. Cumplir con la obligación de confidencialidad de la misma forma y con el mismo cuidado con que se realiza la protección de la información confidencial propia.*

**CLAUSULA QUINTA – Duración.**

*EL EMPLEADO asume la obligación de confidencialidad acordada en el presente Artículo por todo el plazo de la relación laboral y por un plazo adicional de 5 años contados a partir de la extinción del contrato de trabajo.*

**CLAUSULA SEXTA - Devolución de la información.**

*En caso de terminación de la prestación del servicio por cualquier causa, EL EMPLEADO se obliga, a reintegrar o destruir, según le solicite LA INSTITUCION por escrito, toda la documentación e información que le haya sido suministrada y todo otro material o documento que incorpore o refleje Información Confidencial, a la que haya tenido acceso y que conserve EL EMPLEADO. La entrega de la documentación se deberá efectuar en un plazo no mayor a diez (10) días calendario siguiente a la solicitud de entrega de tal documentación por parte de LA INSTITUCION.*

*Igualmente, cualquier Información Confidencial mantenida en computadoras, medios magnéticos o cualquier otro similar, será destruida si así es requerido por LA INSTITUCION. Una vez devuelta y destruida la mencionada documentación, EL EMPLEADO hará constar mediante comunicación escrita que no se encuentra en su poder ningún otro documento sujeto a la obligación de confidencialidad aquí establecida.*

*En caso de EL EMPLEADO no cumpla con la devolución o la destrucción de la información dentro del plazo establecido en la presente Cláusula, LA INSTITUCION queda facultada para accionar por los daños y perjuicios efectivamente ocasionados, así como para constituirse en parte querellante en denuncia penal contra EL EMPLEADO.*

**CLAUSULA SEPTIMA - Clausula penal**

*Yustman, Mauricio Ezequiel*

*Se deja constancia que la violación o el incumplimiento de la obligación de confidencialidad a cargo de EL EMPLEADO podrá dejarlo incurso en el delito de violación de secreto tipificado en el Artículo 156 del Código Penal de la Nación, siendo facultad de LA INSTITUCION formular la denuncia del caso y constituirse en parte querellante.*

#### **CLAUSULA OCTAVA - Compensación. Resarcimiento.**

*Queda expresamente aclarado que la remuneración que EL EMPLEADO percibe de LA FUNDACION, compensa a las obligaciones de confidencialidad, aclaradas en este documento. De igual forma, queda expresamente convenido que todo incumplimiento total y/o parcial imputable al EMPLEADO con relación a las obligaciones de confidencialidad asumidas por el presente, facultará a LA INSTITUCION para disponer la extinción del contrato de trabajo con justa causa. Así mismo LA INSTITUCION queda facultada para accionar por los daños y perjuicios efectivamente ocasionados, así como para constituirse en parte querellante en denuncia penal contra EL EMPLEADO.*

#### **CLAUSULA NOVENA - Legislación aplicable.**

*Este Acuerdo se regirá por las leyes de la República Argentina y se interpretará de acuerdo con las mismas.*

*He leído y estudiado de manera detenida los términos y el contenido del anterior Acuerdo de Confidencialidad y manifiesto estar de acuerdo con todas sus condiciones y las acepto en todo su alcance a partir de la fecha”<sup>192</sup>*

#### **7.4 Condiciones de Uso del servicio WIFI**

##### **Condiciones Particulares de Prestación De Servicio de WIFI Del Hospital Dr. Arturo Oñativia**

Las presentes Condiciones Particulares tienen por objeto establecer los términos y condiciones en los que se presta el Servicio WiFi del Hospital Dr. Arturo Oñativia.

El Servicio WiFi se presta exclusivamente al Personal del Hospital en su calidad de usuario final.

El Servicio WiFi del Hospital Dr. Arturo Oñativia consta de la siguiente prestación:

- Servicio de acceso a Internet

##### **Modalidad**

WIFI Básico: Conexión a Internet sin cables por medio de uno o varios puntos de acceso.

Disponibilidad: El servicio es experimental y se presta a modo de pruebas, depende en muchos aspectos de los recursos con que se dispongan.

##### **Equipamiento**

Se dispondrán de routers y puntos de acceso inalámbrico en diferentes lugares del Hospital según sea necesario, en forma progresiva y dependiendo de los recursos disponibles, a criterio de la Institución.

Los equipos de los Usuarios utilizados para conectarse podrán ser tablets, notebooks, celulares, otros.

- De exclusiva propiedad del usuario: equipos personales.
- Equipos proporcionados por el Hospital.

##### **Seguridad, Límites de Uso y/o Responsabilidades**

---

<sup>192</sup> Redactó Dr. Pablo Eredjian, 2008. ACUERDO DE CONFIDENCIALIDAD.

<http://www.argentina.org.ar/iso9001/Documentos%20Direccion%20Ejecutiva/Formularios%20GRI/GRI-04-F02%20Acuerdo%20de%20confidencialidad%20Rev%2000.pdf>. Vigencia: 14/01/2016.

- Por cuestiones de seguridad, la red y configuraciones necesarias para el funcionamiento se mantienen totalmente apartadas de la red interna de la Institución.
- El Hospital Dr. Arturo Oñativia como así también el Sector Informática no asumen ninguna responsabilidad referente al mal uso o daño alguno (hardware o software) que pudiera sufrir cualquiera de los equipos pertenecientes a los usuarios que sean conectados a esta red.
- Se proporcionarán los datos y medios necesarios para poder realizar la conexión; estos serán:
  - Puntos de acceso (Conectividad) y contraseñas de acceso al mismo.
  - Cuenta personal de usuario (usuario y contraseña respectiva).
- **NO** es responsabilidad del Hospital o del Sector Informática la configuración y/o acondicionamiento de los equipos personales de los usuarios para la conexión, tarea que quedará a cargo de sus respectivos dueños o usuarios.
- La cuenta y medios de acceso proporcionados son personales, es decir que el usuario y contraseña proporcionados para el acceso están ligados a una persona y son **intransferibles**. **NO** debiendo ser compartida bajo ningún punto de vista. Cualquier infracción y/o violación de cualquier índole será adjudicada al usuario responsable de la cuenta.
- Debido a que se trata de un proyecto piloto, y cuyo crecimiento y disponibilidad depende de los recursos que se apliquen al mismo:
  - El servicio wifi **NO** debe ser considerado como medio y/o herramienta en cuestiones laborales, para dichos fines la Institución cuenta con una red interna privada y equipos propios exclusivamente proporcionados para tales usos y necesidades.
  - La disponibilidad del servicio wifi no será tomada como **PRIORIDAD** del Sector Informática cuando los recursos tanto de personal como de tiempo y/o equipamiento no sean suficientes para cubrir las tareas **PRIMARIAS** del Hospital.
- El Hospital Dr. Arturo Oñativia y su dirección se reservan el derecho de proporcionar el servicio o denegar el mismo a quien crea necesario sin necesidad de emitir algún tipo de justificación.
- El Hospital Dr. Arturo Oñativia y su dirección **NO** se responsabilizan bajo ningún punto de vista de las faltas o violación a las leyes y/o normas por el uso de este servicio en que los usuarios pudieran incurrir. Siendo las responsabilidades exclusivas y excluyentes del usuario.
- Cualquier infracción o violación a alguna de estas normas será suficiente para determinar la denegación inmediata y baja del servicio.

Yo, \_\_\_\_\_ DNI \_\_\_\_\_ en  
mi carácter de usuario del servicio WIFI del Hospital Dr. Arturo Oñativia, en el día  
\_\_\_\_\_ manifiesto haber leído y comprendido los términos presentados en este  
convenio y me encuentro en total acuerdo con los mismos, asumiendo las responsabilidades y  
obligaciones impuestas y sus consecuentes sanciones.

.....  
Firma del usuario

.....  
Firma Sector Informática

7.5 Guía de buenas prácticas para el uso de contraseñas.

## **Guía de buenas prácticas para la selección y uso de contraseñas<sup>193</sup>**

La protección contra accesos no autorizados, es una tarea que no solo debe ser de gran importancia para los administradores de los sistemas de información. Los usuarios, tienen un papel importante en esta tarea, ya que deben colaborar de manera activa en la protección de los sistemas de información mediante el adecuada selección y uso de contraseñas. El presente documento brinda a los usuarios recomendaciones para una adecuada selección de contraseñas y otorga pautas para el correcto uso de las mismas.

### **1. Características que debe reunir una contraseña para que sea segura**

- A. Personal: cada persona que acceda a un servicio, aplicación o sistema debe tener su propia contraseña.
- B. Secreta: sólo el usuario de la contraseña debe conocerla.
- C. Intransferible: la contraseña no debe ser revelada a ningún tercero para su uso.
- D. Modificable sólo por el titular: el cambio de contraseña, sea cual fuere el motivo, debe ser realizado solo por el usuario titular de la misma.

### **2. Recomendaciones para la selección de contraseñas**

- Es importante la selección de contraseñas “fuertes”. Deben seleccionarse contraseñas con un mínimo de 8 caracteres alfanuméricos y con caracteres especiales (evitar el uso de la letra “ñ”)
- NO utilizar contraseñas que sean palabras fáciles de identificar (palabras del diccionario español, nombres, palabras en otro idioma, apodos, etc.)
- Las contraseñas deben ser fáciles de recordar por el usuario y difíciles de adivinar. Esto es importante para evitar escribir la contraseña en papel o en algún medio no seguro.
- Evitar el uso de contraseñas que consisten en información fáciles de adivinar o que tienen un significado fácilmente deducible. (DNI, teléfono, fecha de nacimiento, dirección, nombre de la empresa, etc.)
- No utilizar caracteres consecutivos (123456, abcdefg, “qwerty”)

A continuación, se brindan ejemplos para una selección adecuada de contraseña:

- ✓ Combinar palabras cortas con algún número o carácter de puntuación: **soy2\_yo3**
- ✓ Usar un acrónimo de alguna frase fácil de recordar: A río Revuelto Ganancia de Pescadores: **ArRGdP**
- ✓ Añadir un número al acrónimo para mayor seguridad: **A9r7R5G3d1P**

---

<sup>193</sup> El documento fue elaborado con información procedente de las siguientes fuentes:

<http://www.segu-info.com.ar/proteccion/clavesseguras.htm> (vigencia 02/06/2016)

[http://wikiracima.larioja.org/images/3/34/Buenas\\_practicas\\_contrase%C3%B1as.pdf](http://wikiracima.larioja.org/images/3/34/Buenas_practicas_contrase%C3%B1as.pdf) (vigencia 02/06/2016)

[https://www.um.es/atika/documentos/Recomendaciones\\_uso\\_contraseñas.pdf](https://www.um.es/atika/documentos/Recomendaciones_uso_contraseñas.pdf) (vigencia 02/06/2016)

[http://www.jefatura.gob.ar/archivos/servicios\\_al\\_ciudadano/Guia\\_practica\\_sobre\\_el\\_uso\\_de\\_contraseñas.pdf](http://www.jefatura.gob.ar/archivos/servicios_al_ciudadano/Guia_practica_sobre_el_uso_de_contraseñas.pdf) (vigencia 02/06/2016)

- ✓ Mejor incluso si la frase no es conocida: Hasta ahora no he Olvidado mi Contraseña: **HaneOmC**
- ✓ Elegir una palabra sin sentido, aunque pronunciable: **taChunda72, AtajulH, Wen2Mar**
- ✓ Realizar reemplazos de letras por signos o números: En Seguridad Más Vale Prevenir que Curar: **35M/Pq<**

### 3. Recomendaciones para el uso de contraseñas.

- Cambiar las contraseñas periódicamente. Es recomendable realizar esto cada 5 meses para evitar mantener la misma contraseña indefinidamente.
- Mantener la confidencialidad de las contraseñas. Las contraseñas son personales y no deben compartirse, por lo tanto, tampoco debe solicitarse contraseñas a otras personas.
- Es recomendable ingresar las contraseñas cuando nadie está observando para así evitar que un tercero “visualice” su contraseña.
- No usar la misma contraseña en diferentes sistemas de comunicación.
- No llevar un registro en papel en donde este la contraseña. Evitar escribir las contraseñas en algún medio (papel/digital) para recordarla.
- Ante la duda o posibilidad de que la confidencialidad de la contraseña esté en peligro, esta de ser cambiada inmediatamente.

#### 7.6 OCS Inventory

OCS Inventory es una herramienta gratuita que permite a los administrados TI, realizar de manera sencilla y rápida un inventario de todo hardware y software de las maquinas conectadas a una red. Esta herramienta permite obtener un inventario con toda la información necesaria y tiene la gran ventaja de actualizarse de manera automática.

OCS Inventory nos permite visualizar en una interfaz web toda la información de nuestro inventario. El esquema de red utilizado por esta herramienta es el siguiente:

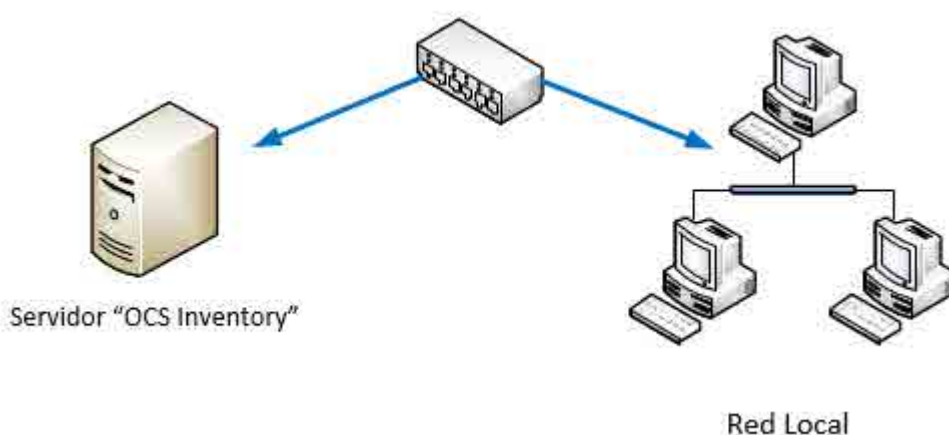


Ilustración 7.6-1

OCS Inventory cuenta con dos herramientas para su funcionamiento:

1. **OCS Inventory Server**: esta herramienta que se instala en el servidor, será el responsable de recabar y administrar la información.
2. **CS Inventory Agent**: Esta aplicación deberá ser instalada en todos los equipos de nuestra red local que deseamos sean inventariados. Esta aplicación recopila la información del equipo (inventario del equipo) para luego proporcionarla al servidor.

Para más información sobre las características de esta herramienta y sus principales funcionalidades dirigirse a <http://www.ocsinventory-ng.org/en/> (página vigente al 07/07/2016)

### **Pruebas realizadas**

Se procedió a realizar la instalación del servidor en una máquina virtual con el propósito de verificar si las funcionalidades ofrecidas por esta herramienta son adecuadas para brindar una solución adecuada al control “Inventario de activos”.

Se realizó la prueba sobre un equipo para verificar la información obtenida al realizar el inventario. También se añadieron campos personalizados a dicho inventario, para que el mismo contenga toda la información requerida por el control “Inventario de activos”. Los resultados se muestran en la siguiente imagen.



The screenshot shows the OCS Inventory web interface. At the top, there's a navigation bar with tabs like 'Home', 'Configuration', 'Inventory', 'Reports', 'Tools', 'Help', and 'About'. Below this, there's a search bar and a table of inventory data. The table has columns for 'Account Info', 'Account Info', 'Account Info', 'Account Info', 'Computer', 'Computer', 'Name', 'System', 'Domain', 'Version', 'Direction', 'Name', and 'Status'. The first row of data shows 'ESTADO', 'NUMERO DE INVENTARIO', 'RESPONSABLE', 'SECTOR/PROGRAMA', 'COMPUTADOR', 'COMPUTER ID', 'NOMBRE USUARIO', 'SISTEMA OPERATIVO', 'DOMINIO', 'VERSION DEL SO', 'DIRECCION MAC', 'NUMERO DE RED', and 'BOTAS'.

| Account Info | Account Info         | Account Info | Account Info    | Computer   | Computer    | Name           | System            | Domain  | Version        | Direction     | Name          | Status |
|--------------|----------------------|--------------|-----------------|------------|-------------|----------------|-------------------|---------|----------------|---------------|---------------|--------|
| ESTADO       | NUMERO DE INVENTARIO | RESPONSABLE  | SECTOR/PROGRAMA | COMPUTADOR | COMPUTER ID | NOMBRE USUARIO | SISTEMA OPERATIVO | DOMINIO | VERSION DEL SO | DIRECCION MAC | NUMERO DE RED | BOTAS  |

Ilustración 7.6-2

Como puede observarse, el registro del inventario fue configurado para llevar la siguiente información sobre el equipo:

- ESTADO: indica el estado del equipo (activo o sin uso)
- NUMERO DE INVENTARIO: en este campo es posible ingresar el número de inventario llevado por patrimonio.
- RESPONSABLE: es posible ingresar el responsable del equipo en cuestión
- COMPUTADOR: nombre del equipo/nombre de red del equipo
- COMPUTER ID: número de identificación del equipo asignado por el software.
- NOMBRE USUARIO: nombre de usuario del equipo
- DOMINIO: grupo de trabajo en el cual se encuentra el equipo
- SISTEMA OPERATIVO: nombre del sistema operativo instalado en el equipo
- VERSION DEL SO
- DIRECCION MAC
- NUMERO DE RED (IP)

Con la configuración realizada, se pudo comprobar que el software propuesto es capaz de llevar la información que se requiere para cumplir con el control “inventario de activos”.

Además de la información previamente detallada, el software propuesto brinda información más detallada sobre el equipo (esto se logra al hacer click en el nombre del computador). A continuación, se muestran las pantallas que detallan la información que es capaz de brindar el software

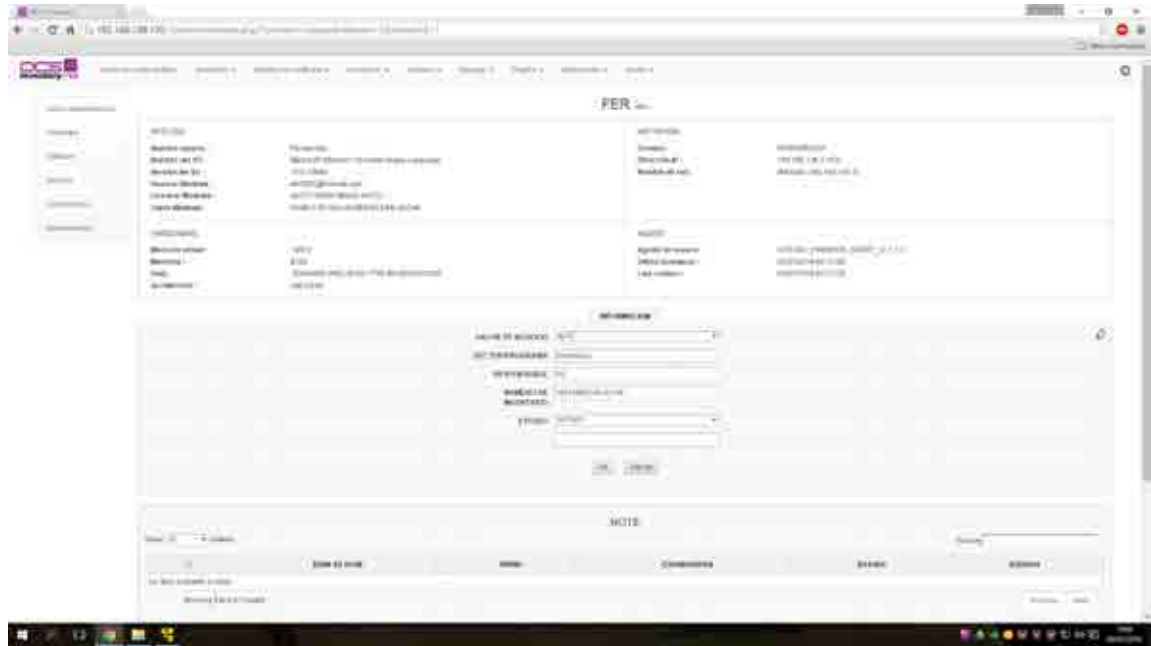


Ilustración 7.6-3

Como puede observarse en la imagen, la información brindada es similar a la obtenida a través del registro de la pantalla inicial. A sí mismo, en la parte superior izquierda es posible visualizar un menú, a través del cual podemos acceder a diferente información sobre el equipo (los más interesantes son hardware, software y devices).

Al seleccionar “hardware” en el menú, nos muestra la siguiente información



**MEMORIA**

| Nombre      | Descripción | Capacidad (MB) | Propiedades | Tip  | Memoria | Numero de memoria | Numero parte |
|-------------|-------------|----------------|-------------|------|---------|-------------------|--------------|
| Memoria RAM | Memoria RAM | 4096           | Memoria RAM | DDR4 | 1       | 1                 | 1            |
| Memoria RAM | Memoria RAM | 4096           | Memoria RAM | DDR4 | 2       | 2                 | 2            |
| Memoria RAM | Memoria RAM | 4096           | Memoria RAM | DDR4 | 3       | 3                 | 3            |
| Memoria RAM | Memoria RAM | 4096           | Memoria RAM | DDR4 | 4       | 4                 | 4            |

**ALMACENAMIENTO**

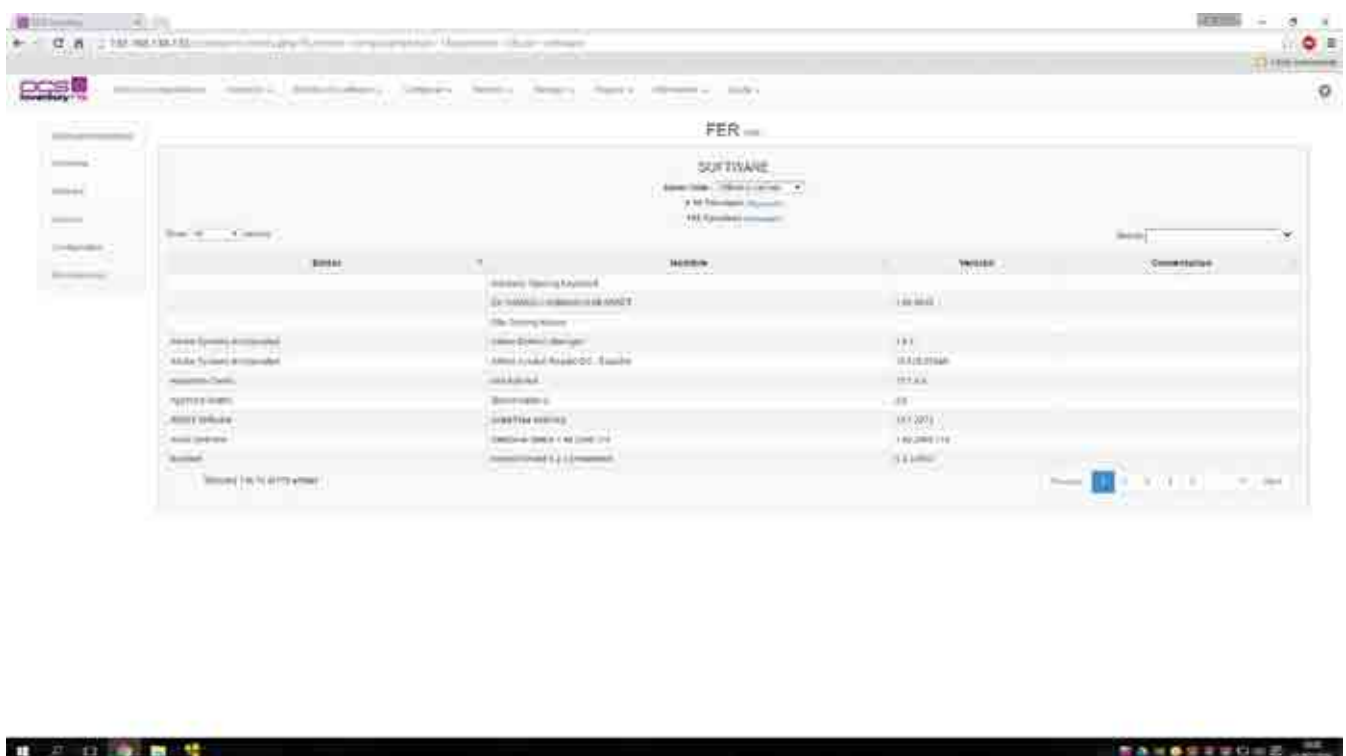
| Nombre     | Formato | Modelo      | Descripción | Tip       | Tamaño del disco (MB) | Numero parte | Formateo |
|------------|---------|-------------|-------------|-----------|-----------------------|--------------|----------|
| Disco duro | NTFS    | ST5000LX007 | Disco duro  | Hard-disk | 500000                | 1            | 1        |
| Disco duro | NTFS    | ST5000LX007 | Disco duro  | Hard-disk | 500000                | 2            | 2        |

**DISCOS**

| Letra | Tip  | Sistema de archivos | Libre (MB) | Total (MB) | Capacidad |
|-------|------|---------------------|------------|------------|-----------|
| C:    | NTFS | NTFS                | 480000     | 500000     | 500000    |
| D:    | NTFS | NTFS                | 480000     | 500000     | 500000    |

Ilustración 7.6-4

Al seleccionar “software” en el menú, nos muestra la siguiente información



**SOFTWARE**

| Nombre            | Version    | Descripción       |
|-------------------|------------|-------------------|
| Microsoft Windows | 10.0.17134 | Microsoft Windows |
| Microsoft Windows | 10.0.17134 | Microsoft Windows |
| Microsoft Windows | 10.0.17134 | Microsoft Windows |
| Microsoft Windows | 10.0.17134 | Microsoft Windows |
| Microsoft Windows | 10.0.17134 | Microsoft Windows |
| Microsoft Windows | 10.0.17134 | Microsoft Windows |
| Microsoft Windows | 10.0.17134 | Microsoft Windows |
| Microsoft Windows | 10.0.17134 | Microsoft Windows |
| Microsoft Windows | 10.0.17134 | Microsoft Windows |
| Microsoft Windows | 10.0.17134 | Microsoft Windows |

Ilustración 7.6-5

Al seleccionar “devices” en el menú, nos muestra la siguiente información

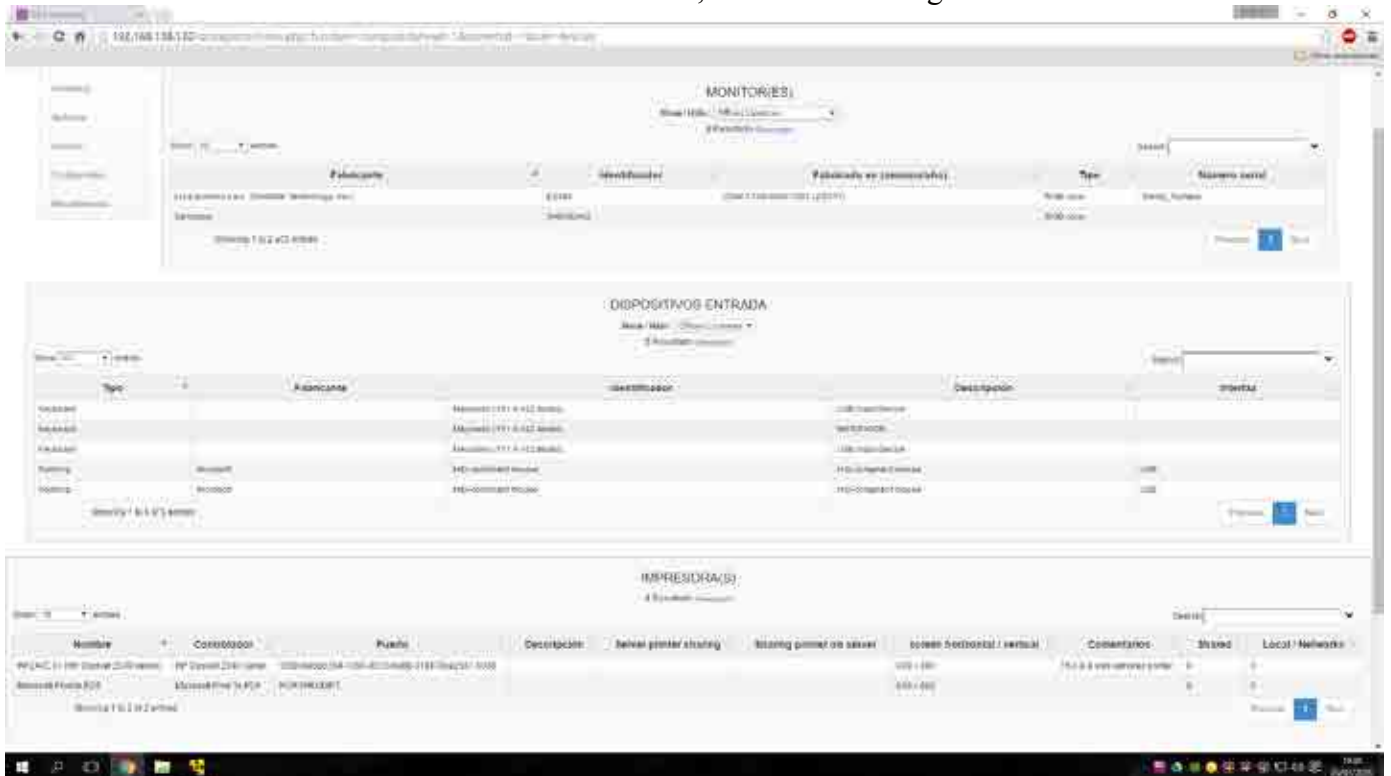


Ilustración 7.6-6

## 7.7 Nomenclador Patrimonio.

| NOMENCLADOR DE BIENES PATRIMONIALES |       |           |     |         |             |                                       |
|-------------------------------------|-------|-----------|-----|---------|-------------|---------------------------------------|
| CLASE                               | Grupo | Sub-Grupo | CTA | Especie | Sub-Especie | DESCRIPCION                           |
| 04                                  | 02    | 08        | 15  | 001     | 00          | ABACO, CONTADOR                       |
| 04                                  | 02    | 08        | 01  | 001     | 00          | ABECEDARIO DE METAL Y NUMEROS         |
| 04                                  | 02    | 08        | 02  | 000     | 00          | ABEGAMIA PARA ANESTESIA               |
| 04                                  | 02    | 02        | 01  | 127     | 00          | ABLANDADORA                           |
| 04                                  | 02    | 04        | 07  | 001     | 00          | ABRATOR                               |
| 04                                  | 02    | 02        | 01  | 001     | 00          | ABOVEADORA                            |
| 04                                  | 02    | 03        | 01  | 001     | 00          | ABPAZADERA                            |
| 04                                  | 02    | 04        | 06  | 001     | 00          | ABREBOCA DE USO ODONTOLOGICO          |
| 04                                  | 02    | 04        | 07  | 002     | 00          | ABREBOCA USO MEDICO Y VETERINARIO     |
| 04                                  | 02    | 03        | 01  | 002     | 00          | ABRELATAS USO TALLER                  |
| 04                                  | 02    | 03        | 01  | 003     | 00          | ABRIDOR USO TALLER Y VARIOS           |
| 04                                  | 02    | 02        | 01  | 002     | 00          | ABRIDORA                              |
| 04                                  | 02    | 04        | 02  | 072     | 00          | ABRILLANTADORA                        |
| 04                                  | 02    | 02        | 01  | 325     | 00          | ABROCHADORA                           |
| 04                                  | 02    | 03        | 01  | 004     | 00          | ACANALADOR                            |
| 04                                  | 02    | 02        | 01  | 003     | 00          | ACANALADORA                           |
| 04                                  | 02    | 04        | 07  | 003     | 00          | ACANTABOLO                            |
| 04                                  | 02    | 04        | 02  | 137     | 00          | ACCESORIOS EQUIPO DE AUDIO            |
| 04                                  | 02    | 04        | 04  | 031     | 00          | ACCESORIOS PILETROGRAFOS              |
| 04                                  | 02    | 04        | 02  | 124     | 00          | ACCESORIOS VARIOS                     |
| 04                                  | 02    | 04        | 03  | 017     | 00          | COMPUTACION (ACCESORIOS VARIOS)       |
| 04                                  | 02    | 03        | 01  | 002     | 00          | ACEITERA DE TALLER                    |
| 04                                  | 02    | 02        | 01  | 004     | 00          | ACEPILLADORA                          |
| 04                                  | 02    | 03        | 01  | 005     | 00          | ACHECADUR                             |
| 04                                  | 02    | 04        | 01  | 002     | 00          | ACIDIMETRO                            |
| 04                                  | 02    | 04        | 01  | 001     | 00          | ACIMUTAL                              |
| 04                                  | 02    | 01        | 03  | 020     | 00          | ACONDICIONADOR DE AIRE                |
| 04                                  | 02    | 02        | 01  | 006     | 00          | ACONDICIONADORA                       |
| 04                                  | 02    | 02        | 01  | 006     | 00          | ACONDICIONADORA                       |
| 04                                  | 02    | 05        | 04  | 001     | 00          | ACOFIADO - CARRETONES                 |
| 04                                  | 02    | 04        | 05  | 003     | 00          | ACORDEON A PIANO                      |
| 04                                  | 02    | 04        | 01  | 003     | 00          | AGTINOMETRO                           |
| 04                                  | 02    | 07        | 01  | 001     | 00          | ACUARELAS, BELLAS ARTES               |
| 04                                  | 02    | 02        | 01  | 005     | 00          | ACUMULADORA                           |
| 04                                  | 02    | 04        | 07  | 217     | 00          | ADENOCOMO                             |
| 04                                  | 02    | 01        | 02  | 000     | 00          | ADORNOS                               |
| 04                                  | 02    | 01        | 02  | 006     | 00          | ADORNOS-TINAJAS                       |
| 04                                  | 02    | 01        | 03  | 015     | 00          | AEROCARGADOR                          |
| 04                                  | 02    | 04        | 04  | 001     | 00          | AEROGRAFO                             |
| 04                                  | 02    | 04        | 01  | 004     | 00          | AEROMETRO                             |
| 04                                  | 02    | 04        | 07  | 004     | 00          | AEROPLANO PARA FRACTURAS              |
| 04                                  | 02    | 03        | 01  | 006     | 00          | AFILADOR USO TALLER Y VS.             |
| 04                                  | 02    | 02        | 01  | 007     | 00          | AFILADORA - AMOLADORA                 |
| 04                                  | 02    | 02        | 01  | 016     | 00          | AFILADORA - AMOLADORA                 |
| 04                                  | 02    | 04        | 01  | 005     | 00          | AFORADOR                              |
| 04                                  | 02    | 06        | 02  | 093     | 00          | AGARRADERA PARA APLICACION CIENTIFICA |
| 04                                  | 02    | 08        | 04  | 008     | 00          | AGENDA                                |
| 04                                  | 02    | 04        | 06  | 001     | 00          | AGITADOR                              |
| 04                                  | 02    | 02        | 01  | 008     | 00          | AGITADORA                             |
| 04                                  | 02    | 04        | 07  | 218     | 00          | AGLUNOSTINOSCOPIO                     |
| 04                                  | 02    | 04        | 01  | 006     | 00          | ALUTINOMETRO                          |
| 04                                  | 02    | 08        | 02  | 000     | 00          | AGRAFES                               |
| 04                                  | 02    | 01        | 01  | 007     | 00          | AGUANTADOR                            |
| 04                                  | 02    | 06        | 02  | 001     | 00          | AGUJA USO MEDICO Y VETERINARIO        |
| 04                                  | 02    | 08        | 01  | 043     | 00          | AGUJA USO TALLER                      |
| 04                                  | 02    | 06        | 02  | 002     | 00          | AGUJAS USO LABORATORIO                |
| 04                                  | 02    | 02        | 01  | 009     | 00          | AGUJERADORA                           |
| 04                                  | 02    | 08        | 03  | 001     | 00          | AHUMADOR PARA ABEJAS                  |
| 04                                  | 02    | 03        | 01  | 009     | 00          | AJUSTA - FORMA                        |
| 04                                  | 02    | 03        | 01  | 008     | 00          | AJUSTADOR                             |
| 04                                  | 02    | 01        | 01  | 090     | 00          | ALACENA                               |
| 04                                  | 02    | 02        | 03  | 001     | 00          | ALAMBQUE DE USO INDUSTRIAL            |
| 04                                  | 02    | 04        | 06  | 002     | 00          | ALAMBQUE USO LABORATORIO              |
| 04                                  | 02    | 08        | 01  | 044     | 00          | ALAMBRE                               |
| 04                                  | 02    | 08        | 03  | 009     | 00          | ALAMBRE PIELERO Y OTROS               |
| 04                                  | 02    | 08        | 02  | 091     | 00          | ALAMBRE PARA TRAUMATOLOGIA            |
| 04                                  | 02    | 08        | 05  | 016     | 00          | ALARMA                                |
| 04                                  | 02    | 06        | 14  | 001     | 00          | ALBA USO RELIGIOSO                    |
| 04                                  | 02    | 07        | 03  | 005     | 00          | ALBUM                                 |
| 04                                  | 02    | 04        | 01  | 007     | 00          | ALBUMINOMETRO                         |
| 04                                  | 02    | 04        | 07  | 005     | 00          | ALBUMOCRAFO                           |

## 7.8 Contrato del Servicio de Seguridad y Vigilancia

**SECRETARIA** **CONTRATO DE SERVICIO DE SEGURIDAD Y VIGILANCIA.**

Entre el "HOSPITAL DE AUTOGESTION Dr. ARTURO OÑATIVIA", representado por su Gerente General Dr. MARCELO NALLAR, con domicilio en E. Paz Chain 36 en adelante denominado "EL HOSPITAL", por una parte y por la otra, la "AGENCIA DE VIGILANCIA PRIVADA [REDACTED]", representada y obligada por su Director [REDACTED] conjuntamente con el titular y Sub-Director Técnico de la entidad, [REDACTED] con domicilio legal en [REDACTED], ambos de la Ciudad de Salta, convienen en celebrar el presente Contrato de Locación de Servicios, que se sujetará a las siguientes cláusulas:

1º) "LA AGENCIA" brindará al "HOSPITAL" el Servicio de Seguridad y Vigilancia en las instalaciones y adyacencias que esta última posee en el domicilio citado, con los siguientes objetivos, entre otros, de: Prevenir robos y hurtos. Controlar movimiento de entradas y salidas de personal interno, tercerizados, visitas, transporte de insumos, carga y descarga de mercancías y su documentación respaldatoria. Recorrer todos los sectores internos y perimetrales del Hospital, observando el funcionamiento de los servicios internos. Controlar la hermeticidad de los depósitos y consultorios. Controlar el transporte interno de maquinarias y herramientas y las provenientes del exterior. Proteger y brindar seguridad a los pacientes, a las personas que ingresen como visita y dependientes del Organismo. Como también el control de bienes y útiles. Entre las partes se implementará el uso de un "LIBRO DE NOVEDADES", foliado, como medio práctico y dinámico de determinar y variar las funciones específicas a cumplir. Que, al encontrarse pronto de implementarse el Rol de Evacuación del Hospital, la Agencia y sus dependientes se comprometen a tener activa presencia y participación en sus lineamientos y funcionamiento, instrucciones que se volcarán en el "Libro de Novedades".

2º) El Servicio será brindado por [REDACTED] Vigiladores desde hs [REDACTED] [REDACTED] uno apostado en [REDACTED] [REDACTED] en el [REDACTED] 0 [REDACTED] Vigiladores, [REDACTED] [REDACTED]. Tendrán a su cargo además, la atención de la caldera y en caso de un corte de energía eléctrica, observar que el grupo electrógeno encienda de manera automática. Ante un eventual desperfecto de los sistemas, deberán llamar en el acto al Técnico Sr. [REDACTED].

3º) El desempeño de la Agencia y su Personal de Vigilancia se ajustará a los parámetros que se establezcan de común acuerdo entre las partes, a la Ley 7273/04 Régimen sobre Empresas de Vigilancia Privada, a los principios del Derecho Privado y Público y los que se encuentren volcados en este

Contrato y en el LIBRO DE NOVEDADES, tendientes a proteger los bienes patrimoniales, instalaciones y vigilancia de personas y movimientos, actuando en todo momento con actitud preventiva y disuasiva, tendiente a evitar la comisión de hechos ilícitos o de cualquier otra naturaleza que vaya en perjuicio de personas o del HOSPITAL o que perturben el normal desenvolvimiento de los profesionales, enfermeros y personal administrativo. Se tendrá especial respeto y consideración con los pacientes, sean éstos internados o ambulatorios. Siéndole prohibido al Personal de Vigilancia el acceso a Sala de Recuperación, a Cirugía y a las habitaciones de los internados, salvo justificadas razones de fuerza mayor. Requiriéndose de dicho Personal, una actitud totalmente profesional, no intimando en el trato con terceros, sean éstos compañeros, personal de planta hospitalaria, pacientes o sus familiares, lo que no quita la observancia de una conducta cortés. El Hospital podrá solicitar rotación de personal cuando lo considere necesario. Conforme a conducta laboral y/o personal de los mismos o ante el transcurso de un determinado tiempo, a criterio del Hospital, o bien efectuarlo la Agencia. Esta deberá suministrar los datos personales de cada agente, juntamente con certificado de buena conducta.

4º) El precio del Servicio que abonará EL HOSPITAL, [REDACTED] mes, a [REDACTED]. La facturación, según normas en vigencia, será mensual y la forma de pago a mes vencido. El lugar de pago se establece en calle E. Paz Chain n° 36. Para el caso de producirse variaciones en el salario básico, conforme CCT 507/07 y anexos, se podrá concertar dicho incremento de común acuerdo entre las partes, previo tratamiento y autorización del Consejo de Administración.

5º) El presente Contrato tendrá vigencia por [REDACTED], desde la firma del presente, renovable por igual período previo acuerdo de partes. Previo tratamiento y autorización del Consejo de Administración.

6º) El personal afectado al Servicio que se contrata, tiene exclusiva y única relación laboral con la Agencia de Vigilancia. Respondiendo ésta ante EL HOSPITAL, por acción de repetición, ante una potencial demanda judicial de cualquier tipo de su personal.

7º) La Agencia proveerá al personal afectado al Servicio, el correspondiente uniforme, el que estará siempre en buen estado de conservación y presentación; los elementos, insumos y todo otro accesorio idóneo y adecuado para una correcta y eficiente prestación. Figurando en anexo el detalle del uniforme e identificación y domicilio del personal, el que contará con las habilitaciones correspondientes conforme a las normas legales vigentes. Comprometiéndose la EMPRESA a comunicar, previamente, en caso de cambiar de personal o variar la indumentaria o identificación.

8º) EL HOSPITAL proveerá al personal de vigilancia de un lugar adecuado para que éstos guarden sus elementos de trabajo (Sistema de comunicación

y de iluminación e indumentaria). No debiéndose guardar ni hacer uso de elementos inflamables y/o explosivos, ni tampoco objetos que no sean de estricto uso laboral. (Ej. Celulares, Play station, etc.)

9°) El Personal de Vigilancia recibirá órdenes o instrucciones del Gerente General, Administrativo, de Atención a las Personas, Asesor Letrado y/o del Jefe de Control y Fiscalización de Servicios Generales. En los días sábados, domingos y feriados, del Médico de Guardia y en su defecto, de la Jefatura de Enfermería. Las instrucciones impartidas bajo constancia de firma, serán registradas en el "LIBRO de NOVEDADES" habilitado a tales fines.

10°) El cumplimiento de las leyes impositivas, de Seguro por accidente de trabajo y laborales, aplicables al personal de vigilancia afectado al presente Servicio, estará a cargo exclusivo de la Agencia, relevando expresamente al HOSPITAL, de toda obligación respecto al personal que aquella gerencia.

11°) La dirección, control de horario, asistencia, disciplina del personal y conducción técnica del Servicio, así como la designación, remoción y sustitución del personal destacado, son facultades exclusivas de la Agencia, salvo que, debido a casos de incumplimientos, inobservancia o negligencias por parte del personal, sean solicitados por el HOSPITAL. La Agencia efectuará en forma permanente, la supervisión e inspección del Servicio.

12°) La Agencia informará bimestralmente al Gerente General o Gerente Administrativo, la marcha del presente Servicio y formulará y recibirá las sugerencias que considere necesarias para el perfeccionamiento del mismo; también deberá brindar inmediata información cuando se produzca cualquier novedad. Como también las novedades que se observen a través del sistema de circuito cerrado televisión, cuyas grabaciones diarias como las novedades serán conservadas y estarán disponibles para el Hospital por un plazo mínimo de [REDACTED] días, con su debido resguardo ante la posibilidad de ser bajada en backup por personal de informática del Hospital.

13°) La Agencia "[REDACTED]" asume efectivamente ante EL HOSPITAL, su responsabilidad por accidentes de trabajo en el lugar e itinere que pudiera sufrir cualquiera de los trabajadores integrantes de La Agencia durante la vigencia del Convenio, incluso las responsabilidades derivadas de los accidentes de trabajo o enfermedades profesionales que pudieran afectarlos, sin perjuicio que primariamente pudieran ser atendidos en el Hospital. Al efecto deberá contar con la cobertura aseguradora necesaria conforme lo dispone la legislación y reglamentación laboral y de Riesgo del Trabajo vigente.

14°) En caso de producirse algún evento delictivo que traiga aparejada faltante de bienes debidamente identificados, de propiedad del HOSPITAL, la Agencia deberá responder pecuniariamente hasta la concurrencia del valor de los mismos o proceder a su reposición, en el supuesto de negligencia en el cumplimiento del servicio encomendado. Asimismo, el Hospital pondrá en conocimiento de la Agencia un inventario, en caso de solicitarlo, con los bienes muebles en existencia, indicando el sector donde los mismos se encuentran.

15°) El incumplimiento de cualquiera de las Partes, de las obligaciones respectivas a su cargo, derivadas del presente contrato, faculta a la

otra para declararlo rescindido, sin necesidad de interpelación judicial, siendo suficiente notificación un medio fehaciente, efectuado con siete días de anticipación, salvo razones de fuerza mayor, generándose en ambos casos de rescisión, derecho de indemnización por la extinción anticipada del contrato, a la parte que padezca y demuestre el perjuicio. Asiste a cada parte el derecho de rescindir unilateralmente el convenio, sin expresión de causa, para lo cual deberá comunicar fehacientemente a la otra con 60 días de anticipación.

16°) Para el caso que se presentara alguna controversia derivada de la interpretación o ejecución del presente contrato, privará el objeto del mismo, la buena fe de las partes y lo que verosimilmente se quiso decir y lograr. Con los domicilios especiales constituidos, las partes se someten a la jurisdicción y competencia de los Tribunales Ordinarios de la Ciudad de Salta. El impuesto de sellos será soportado por partes iguales, encontrándose el Hospital eximido de tal obligación.

En prueba de conformidad, se firman dos ejemplares de un mismo tenor y a un solo efecto, en la Ciudad de Salta a [redacted] día del mes de [redacted] de [redacted] Mon [redacted] Año [redacted]

[redacted]

[redacted]

[redacted]

Dr. [redacted]  
Hosp. [redacted] R. [redacted]  
[redacted] Salta

7.9 Contrato de locación de servicio.

CONTRATO DE LOCACION DE SERVICIOS.

Entre el HOSPITAL DE AUTOGESTION "Dr. ARTURO OÑATIVIA", representado por su Gerente General [REDACTED], con domicilio en E. Paz Chain 36 en adelante "EL HOSPITAL" por una parte, y por la otra, [REDACTED], DNI n° [REDACTED], con domicilio en [REDACTED], en adelante "LA CONTRATADA", ambos de la Ciudad de Salta, acuerdan celebrar el presente convenio, sujeto a las siguientes cláusulas:

01.- "EL HOSPITAL" contrata los servicios de [REDACTED] para cumplir tareas inherentes al Programa Estadística como Auxiliar Administrativo en horario matutino, con [REDACTED] horas semanales.

02.- El pago a cargo de "EL HOSPITAL" consistirá en un importe mensual [REDACTED] y contra entrega de recibo.- Siendo a cargo de la contratada sus aportes previsionales.

03.- El presente Convenio tendrá vigencia por [REDACTED], desde [REDACTED] al [REDACTED]- "EL HOSPITAL" se reserva el derecho de rescindirlo, comunicando con 30 días corridos de anticipación, salvo causas que, por las circunstancias impongan la inmediata resolución contractual.

04.- De la misma manera, "LA CONTRATADA" podrá resolver el presente convenio, sin dar razón, comunicándolo fehacientemente con 30 días corridos de anticipación.- Si "LA CONTRATADA" no cumpliera con la notificación en término, el Hospital se reserva el derecho de no abonar los haberes correspondientes al mes que deje de prestar servicios.- En ningún supuesto tendrá derecho a reclamar indemnización alguna.

05.- La falta de presencia de la Contratada a cada día de prestación, dará lugar a la pérdida del porcentaje diario del importe que cobra por mes, que se descontará al momento de efectuar cualquier pago.- Incurriendo en la tercera falta de prestación continuada o cinco alternada, dentro del período de contratación, dará derecho al "HOSPITAL" a tener por finalizado el presente, notificando tal decisión.

06.- El gasto de sellado será proporcional entre las partes.

07.- Las partes constituyen domicilio en los indicados ut-supra para todos los efectos legales y se someten a la Jurisdicción de los Tribunales Ordinarios del Distrito Judicial del Centro con asiento en la Ciudad de Salta, renunciando a cualquier otro que pudiera corresponderles.

En prueba de conformidad, se firman dos ejemplares de igual tenor  
 y a un mismo efecto en la Ciudad de Salta a los [ ] días del mes de [ ]  
 de [ ]

[Redacted Signature]

[Redacted Signature]

## 7.10 SGII (Sistema de gestión de incidentes de seguridad de la información).

### 7.10.1 Diagrama de clases

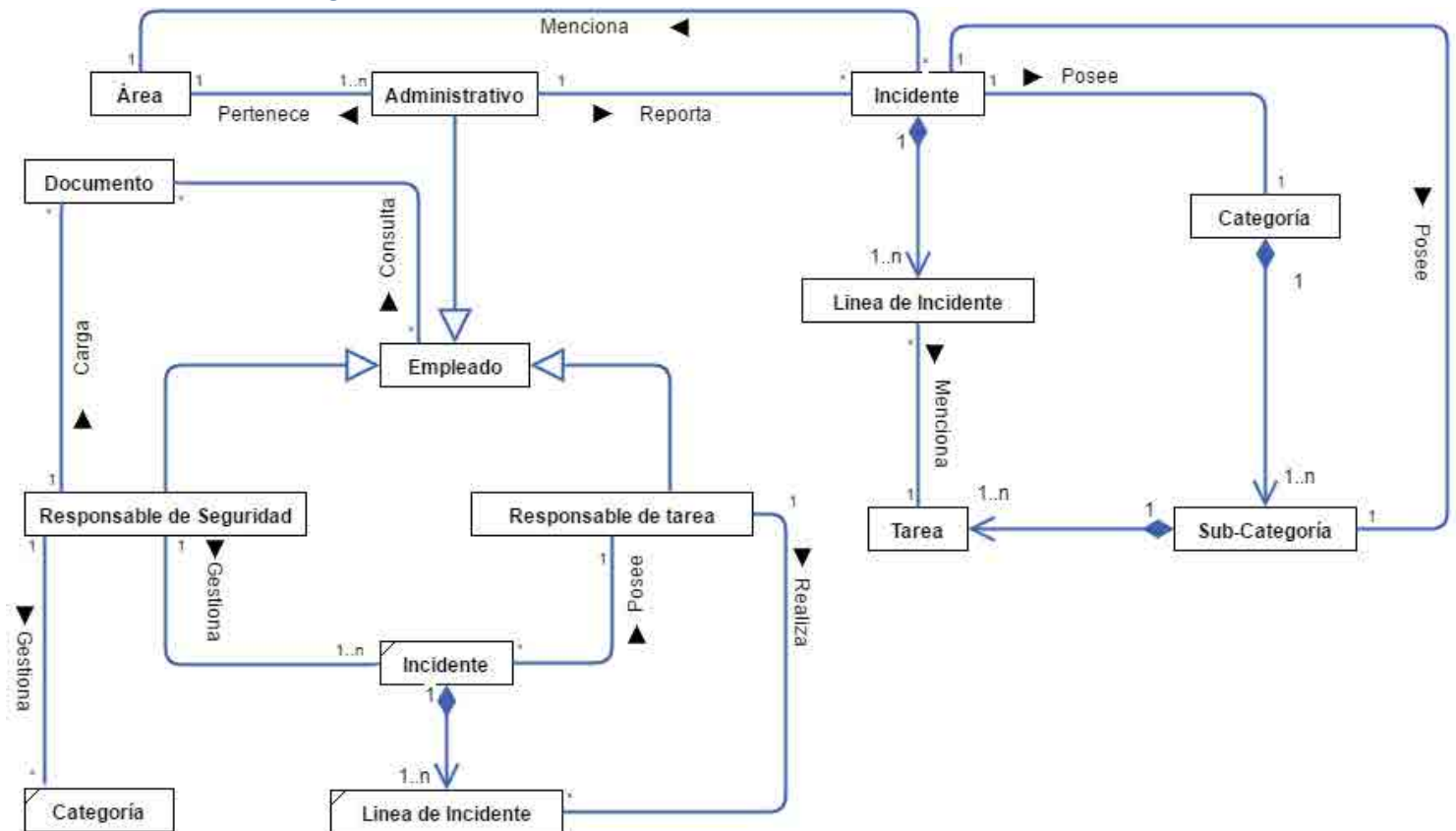


Ilustración 7.10-1

### 7.10.2 Lista de casos de uso

- Validar Usuario
- Registrar Incidente
- Visualizar documentación de Seguridad
- Registrar Usuario
- Recepcionar Incidente
- Gestionar Tareas

Yustman, Mauricio Ezequiel

Pérez Osán, Fernando Javier

- g) Gestionar Incidente
- h) Cargar Documentación de Seguridad
- i) Generar Informe de Incidentes registrados por Sub-Categoría
- j) Generar Informe de Incidentes registrados por Categoría
- k) Generar Informe de Tiempo Total por Sub-Categoría de Incidente
- l) Generar Informe de Tiempo Promedio por Sub-Categoría de Incidente

### 7.10.3 Especificación de los casos de uso

#### 7.10.3.1 Validar usuario

| ID_CU: Validar Usuario                                                                                                              |                         |
|-------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Actor: Personal del Hospital Dr. Arturo Oñativia (Administrativo), Responsable de Seguridad de la Información, Responsable de tarea |                         |
| Pre-Condiciones: <ul style="list-style-type: none"> <li>• Usuario creado</li> <li>• Usuario habilitado</li> </ul>                   |                         |
| Post-Condiciones: <ul style="list-style-type: none"> <li>• Usuario Logeado</li> <li>• Permisos Validados</li> </ul>                 |                         |
| Escenario Principal de Éxito                                                                                                        |                         |
| Actor                                                                                                                               | Sistema                 |
| 1. Iniciar CU                                                                                                                       |                         |
|                                                                                                                                     | 2. Solicitar Usuario    |
|                                                                                                                                     | 3. Solicitar Contraseña |
| 4. Ingresar Usuario                                                                                                                 |                         |
| 5. Ingresar Contraseña                                                                                                              |                         |
|                                                                                                                                     | 6. Validar Usuario      |
|                                                                                                                                     | 7. Validar Contraseña   |
|                                                                                                                                     | 8. Iniciar sesión       |
|                                                                                                                                     | 9. Validar Permisos     |

|                                                |                                                            |
|------------------------------------------------|------------------------------------------------------------|
|                                                | 10. Habilitar opciones permitidas para el Usuario          |
|                                                | 11. Fin de CU                                              |
| Escenario de Alternativas                      |                                                            |
| 6. Validar Usuario (Usuario Incorrecto)        |                                                            |
| Actor                                          | Sistema                                                    |
|                                                | 6.1 Mostrar Error "Usuario o contraseña incorrecto"        |
|                                                | 6.2 Volver al Paso 1                                       |
| 7.A Validar Contraseña (Contraseña Incorrecta) |                                                            |
| Actor                                          | Sistema                                                    |
|                                                | 7.A.1 Mostrar Error "Usuario o contraseña incorrecto"      |
|                                                | 7.A.2 Volver al Paso 1                                     |
| 7.B Validar Usuario (Contraseña caducada)      |                                                            |
| Actor                                          | Sistema                                                    |
|                                                | 7.B.1 Mostrar Mensaje "Debe ingresar una nueva contraseña" |
| 7.B.2 Ingresar nueva Contraseña                |                                                            |
|                                                | 7.B.3 Validar Contraseña                                   |
|                                                | 7.B.4 Actualizar Contraseña                                |
|                                                | 7.B.5 Volver al paso 8                                     |

7.B.3 Validar Usuario (Contraseña no cumple requisitos de seguridad)

| Actor | Sistema                                                  |
|-------|----------------------------------------------------------|
|       | 7.B.3.1 Mostrar Error "Error al comprobar la contraseña" |
|       | 7.B.3.2 Volver al paso 7.B.2                             |

Tabla 7.10-1

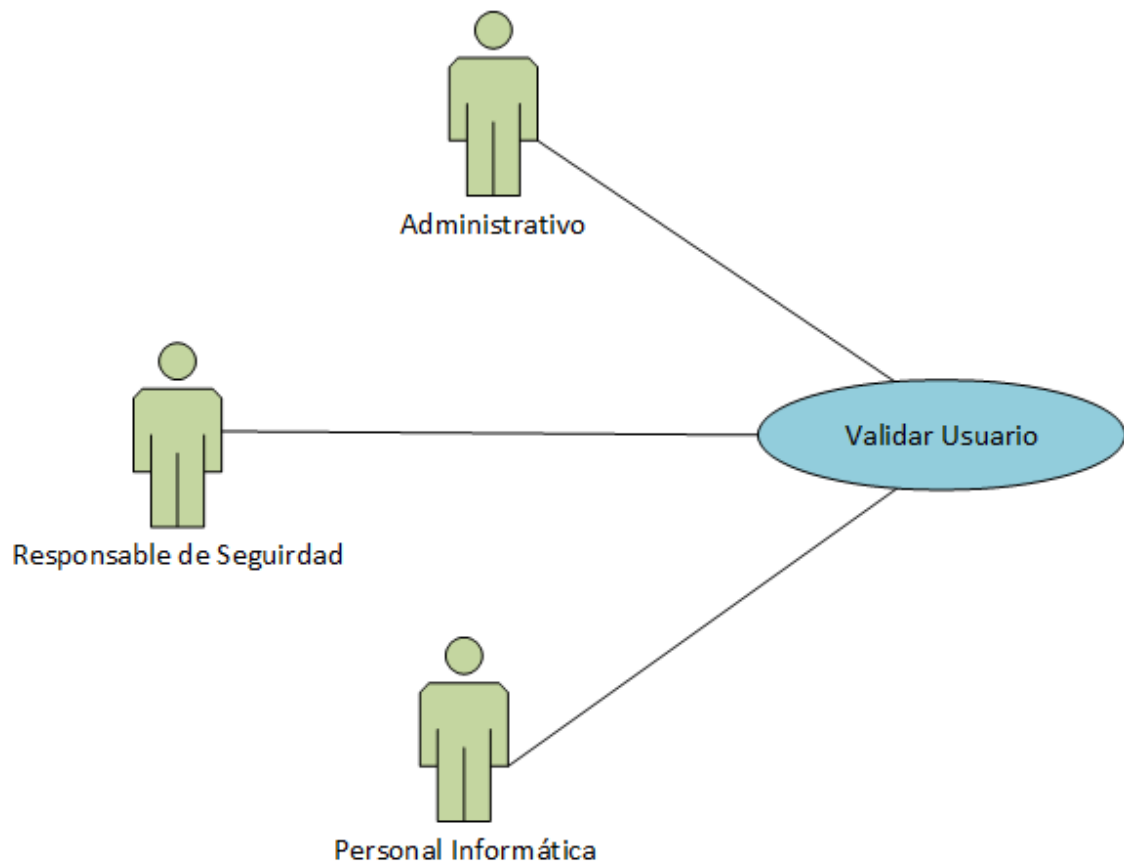


Ilustración 7.10-2

7.10.3.2 Registrar Incidente

ID\_CU: Registrar Incidente

Actor: Personal del Hospital Dr. Arturo Oñativia, Responsable de Seguridad de la Información, Personal de sector de Sistemas Informáticos

Pre-Condiciones:

- Usuario Logeado

|                                                                                                                       |                                                                      |
|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>Permisos Validados</li> </ul>                                                  |                                                                      |
| Post-Condiciones: <ul style="list-style-type: none"> <li>Incidente registrado en estado <i>"Pendiente"</i></li> </ul> |                                                                      |
| Escenario Principal de Éxito                                                                                          |                                                                      |
| Actor                                                                                                                 | Sistema                                                              |
| 1. Iniciar CU                                                                                                         |                                                                      |
|                                                                                                                       | 2. Solicitar datos de Incidente                                      |
| 3. Ingresar titulo descriptivo                                                                                        |                                                                      |
| 4. Ingresar Fecha                                                                                                     |                                                                      |
| 5. Ingresar breve descripción del Incidente                                                                           |                                                                      |
| 6. Confirmar Incidente                                                                                                |                                                                      |
|                                                                                                                       | 7. Validar Confirmación                                              |
|                                                                                                                       | 8. Registrar Incidente en estado <i>"Pendiente"</i>                  |
|                                                                                                                       | 9. Enviar notificación al Responsable de Seguridad de la Información |
|                                                                                                                       | 10. Fin CU                                                           |
| Escenario de Alternativas                                                                                             |                                                                      |
| 6.A Confirmar Incidente (Cancelar)                                                                                    |                                                                      |
| Actor                                                                                                                 | Sistema                                                              |
| 6.A.1 Cancelar Operación                                                                                              |                                                                      |
|                                                                                                                       | 6.A.2 Cancelar Operación                                             |
|                                                                                                                       | 6.A.3 Fin CU                                                         |

| 6.B Confirmar Incidente (Modificar Datos del Incidente) |                                   |
|---------------------------------------------------------|-----------------------------------|
| Actor                                                   | Sistema                           |
|                                                         | 6.B.1 Mostrar datos del Incidente |
| 6.B.2 Modificar datos del Incidente                     |                                   |
|                                                         | 6.B.3 Volver al paso 6            |

Tabla 7.10-2

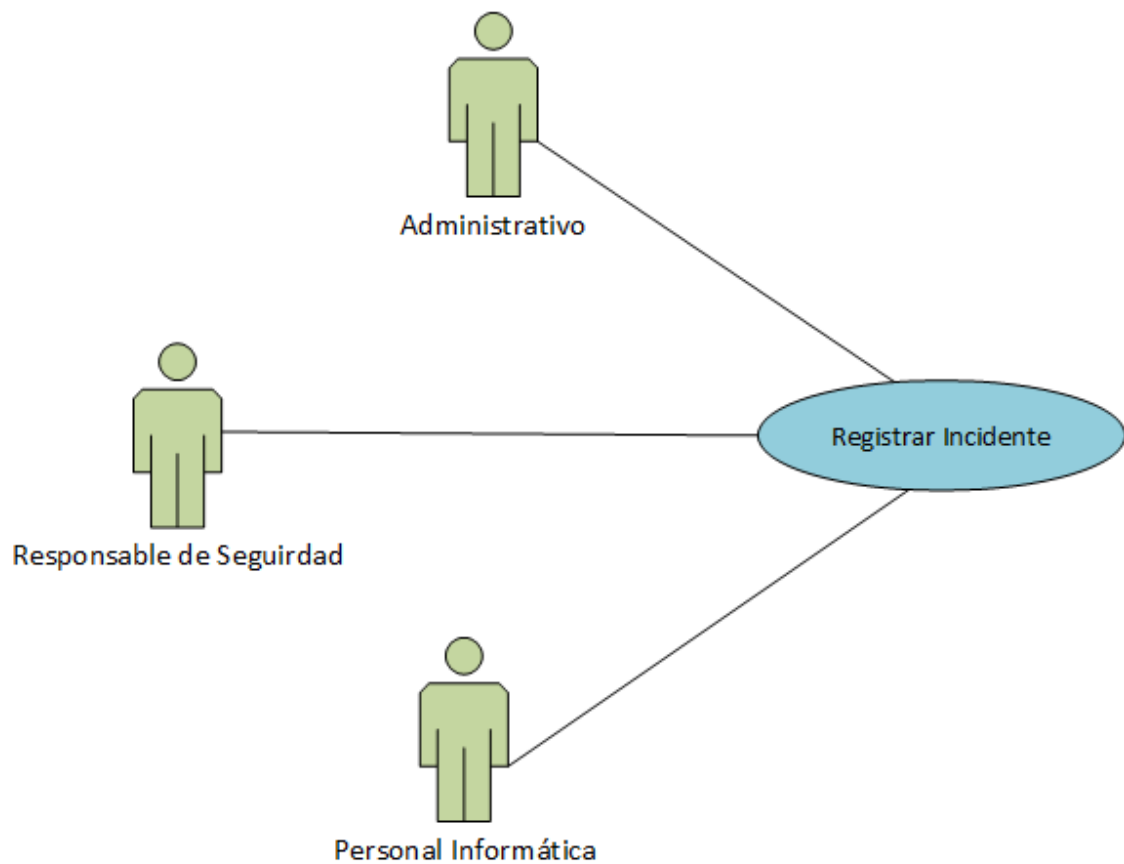


Ilustración 7.10-3

### 7.10.3.3 Visualizar documentación de Seguridad

|                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------------------|
| ID_CU: Visualizar documentación de Seguridad                                                                                              |
| Actor: Personal del Hospital Dr. Arturo Oñativia, Responsable de Seguridad de la Información, Personal de sector de Sistemas Informáticos |
| Pre-Condiciones: <ul style="list-style-type: none"> <li>● Usuario Logeado</li> </ul>                                                      |

|                                                                                                                                        |                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Permisos Validados</li> <li>• Documentación de Seguridad de la Información cargado</li> </ul> |                                                                 |
| Post-Condiciones: <ul style="list-style-type: none"> <li>• Documento Descargado</li> </ul>                                             |                                                                 |
| Escenario Principal de Éxito                                                                                                           |                                                                 |
| Actor                                                                                                                                  | Sistema                                                         |
| 1. Iniciar CU                                                                                                                          |                                                                 |
|                                                                                                                                        | 2. Mostrar listado de Documentos de Seguridad de la Información |
| 3. Seleccionar Documento                                                                                                               |                                                                 |
| 4. Confirmar Descarga                                                                                                                  |                                                                 |
|                                                                                                                                        | 5. Validar confirmación                                         |
|                                                                                                                                        | 6. Enviar Documento                                             |
|                                                                                                                                        | 7. Fin CU                                                       |
| Escenario de Alternativas                                                                                                              |                                                                 |
| 4. Confirmar Descarga (Cancelar)                                                                                                       |                                                                 |
| Actor                                                                                                                                  | Sistema                                                         |
| 4.1 Cancelar Operación                                                                                                                 |                                                                 |
|                                                                                                                                        | 4.2 Cancelar Operación                                          |
|                                                                                                                                        | 4.3 Fin CU                                                      |

Tabla 7.10-3

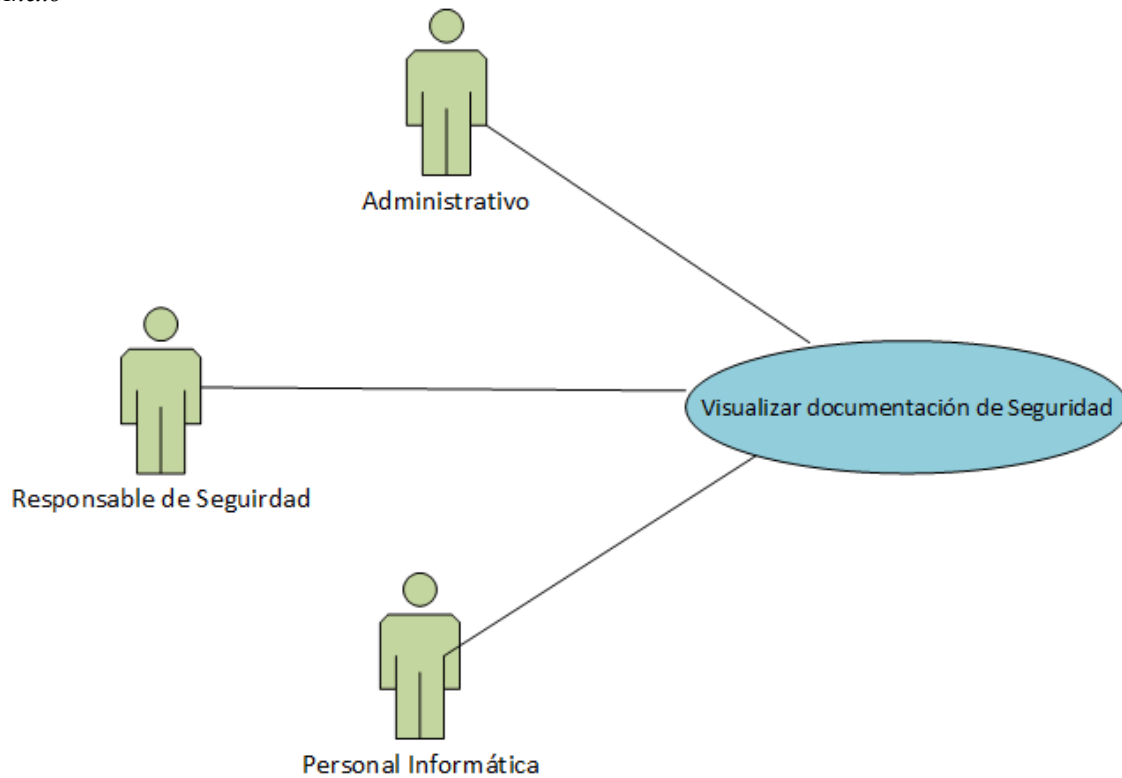


Ilustración 7.10-4

#### 7.10.3.4 Registrar Usuario

|                                                                                                                    |                                |
|--------------------------------------------------------------------------------------------------------------------|--------------------------------|
| ID_CU: Registrar Usuario                                                                                           |                                |
| Actor: Responsable de Seguridad de la Información, Personal de sector de Sistemas Informáticos                     |                                |
| Pre-Condiciones: <ul style="list-style-type: none"> <li>• Usuario Logeado</li> <li>• Permisos Validados</li> </ul> |                                |
| Post-Condiciones: <ul style="list-style-type: none"> <li>• Usuario Creado</li> </ul>                               |                                |
| Escenario Principal de Éxito                                                                                       |                                |
| Actor                                                                                                              | Sistema                        |
| 1. Iniciar CU                                                                                                      |                                |
|                                                                                                                    | 2. Solicitar Datos del Usuario |
| 3. Ingresar nombre de Usuario                                                                                      |                                |

|                                                 |                                       |
|-------------------------------------------------|---------------------------------------|
| 4. Ingresar Contraseña                          |                                       |
| 5. Ingresar datos personales del Usuario        |                                       |
| 6. Seleccionar Sector/Programa al que pertenece |                                       |
| 7. Confirmar Usuario                            |                                       |
|                                                 | 8. Validar Usuario                    |
|                                                 | 9. Registrar Usuario                  |
|                                                 | 10. Marcar contraseña como “Caducada” |
|                                                 | 11. Fin de CU                         |

#### Escenario de Alternativas

##### 7.A Confirmar Usuario (Cancelar)

| Actor                    | Sistema                  |
|--------------------------|--------------------------|
| 7.A.1 Cancelar Operación |                          |
|                          | 7.A.2 Cancelar Operación |
|                          | 7.A.3 Fin CU             |

##### 7.B Confirmar Usuario (Modificar Datos del Usuario)

| Actor                             | Sistema                         |
|-----------------------------------|---------------------------------|
|                                   | 7.B.1 Mostrar datos del Usuario |
| 7.B.2 Modificar datos del Usuario |                                 |
|                                   | 7.B.3 Volver al paso 7          |

##### 8.A Validar Usuario (Nombre de Usuario existente)

| Actor                             | Sistema                                          |
|-----------------------------------|--------------------------------------------------|
|                                   | 8.A.1 Mostrar Error "Nombre de Usuario repetido" |
|                                   | 8.A.2 Mostrar datos del Usuario                  |
| 8.A.2 Modificar Nombre de Usuario |                                                  |
|                                   | 8.A.3 Volver al paso 7                           |

8.B Validar Usuario (Contraseña no cumple requisitos de seguridad)

| Actor                      | Sistema                                                |
|----------------------------|--------------------------------------------------------|
|                            | 8.B.1 Mostrar Error "Error al comprobar la contraseña" |
|                            | 8.B.2 Mostrar datos del Usuario                        |
| 8.B.2 Modificar Contraseña |                                                        |
|                            | 8.A.3 Volver al paso 7                                 |

Tabla 7.10-4

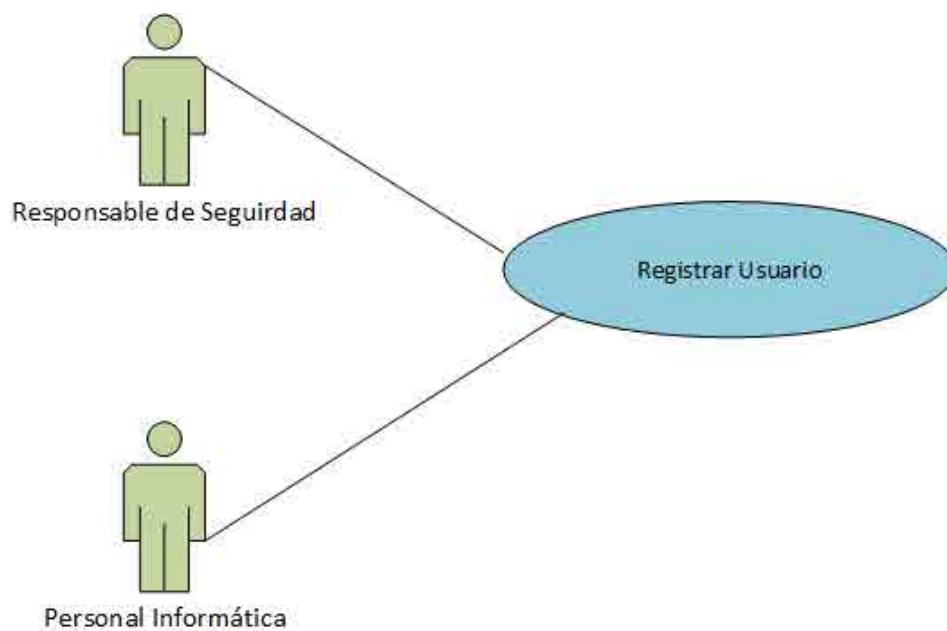


Ilustración 7.10-5

|                                                                                                                                                                                                                                                                            |                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| ID_CU: Recepcionar Incidente                                                                                                                                                                                                                                               |                                                        |
| Actor: Responsable de Seguridad de la Información                                                                                                                                                                                                                          |                                                        |
| Pre-Condiciones: <ul style="list-style-type: none"> <li>• Usuario Logeado</li> <li>• Permisos Validados</li> <li>• Categoría de Incidente cargada</li> <li>• Sub-Categoría de Incidente cargada</li> <li>• Tareas para resolver Incidente categorizado cargadas</li> </ul> |                                                        |
| Post-Condiciones: <ul style="list-style-type: none"> <li>• Incidente en estado “En Proceso”</li> </ul>                                                                                                                                                                     |                                                        |
| Escenario Principal de Éxito                                                                                                                                                                                                                                               |                                                        |
| Actor                                                                                                                                                                                                                                                                      | Sistema                                                |
| 1. Iniciar CU                                                                                                                                                                                                                                                              |                                                        |
|                                                                                                                                                                                                                                                                            | 2. Mostrar listado de Incidentes en Estado “Pendiente” |
| 3. Seleccionar Incidente                                                                                                                                                                                                                                                   |                                                        |
|                                                                                                                                                                                                                                                                            | 4. Mostrar datos del Incidente                         |
|                                                                                                                                                                                                                                                                            | 5. Mostrar Categorías                                  |
| 6. Seleccionar Categoría                                                                                                                                                                                                                                                   |                                                        |
|                                                                                                                                                                                                                                                                            | 7. Mostrar Sub-Categorías                              |
| 8. Seleccionar Sub-Categorías                                                                                                                                                                                                                                              |                                                        |
|                                                                                                                                                                                                                                                                            | 9. Mostrar tareas a realizar                           |
|                                                                                                                                                                                                                                                                            | 10. Mostrar Responsables                               |
| 11. Seleccionar Responsable                                                                                                                                                                                                                                                |                                                        |

|               |                                                    |
|---------------|----------------------------------------------------|
| 12. Confirmar |                                                    |
|               | 13. Validar                                        |
|               | 14. Actualizar datos del Incidente                 |
|               | 15. Actualizar estado del Incidente a "En Proceso" |
|               | 16. Fin de CU                                      |

Escenario de Alternativas

3. Seleccionar Incidente (Cancelar Selección)

|                        |                      |
|------------------------|----------------------|
| Actor                  | Sistema              |
| 3.1 Cancelar Selección |                      |
|                        | 3.2 Volver al paso 3 |

6. Seleccionar Categoría(Cancelar Selección)

|                        |                      |
|------------------------|----------------------|
| Actor                  | Sistema              |
| 6.1 Cancelar Selección |                      |
|                        | 6.2 Volver al paso 5 |

11. Seleccionar Responsable (Cancelar Selección)

|                         |                       |
|-------------------------|-----------------------|
| Actor                   | Sistema               |
| 11.1 Cancelar Selección |                       |
|                         | 11.2 Volver al paso 6 |

12.A Confirmar (Cancelar)

| Actor                                          | Sistema                   |
|------------------------------------------------|---------------------------|
| 12.A.1 Cancelar Operación                      |                           |
|                                                | 12.A.2 Cancelar Operación |
|                                                | 12.A.3 Fin CU             |
| 12.B Confirmar (Modificar datos del Incidente) |                           |
| Actor                                          | Sistema                   |
| 12.B.1 Volver al paso 5                        |                           |

Tabla 7.10-5

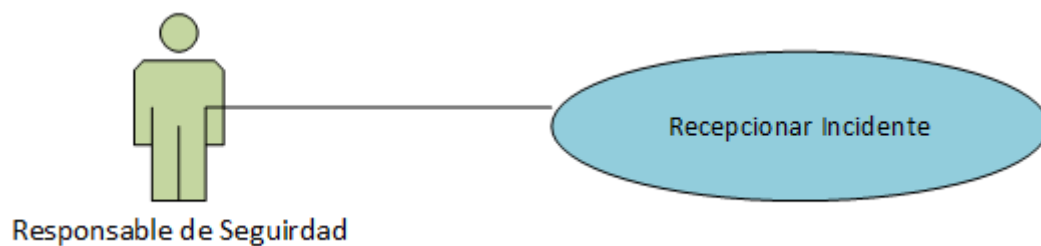


Ilustración 7.10-6

#### 7.10.3.6 Gestionar Tareas

| ID_CU: Gestionar Tareas                                                                                            |         |
|--------------------------------------------------------------------------------------------------------------------|---------|
| Actor: Responsable de Seguridad de la Información                                                                  |         |
| Pre-Condiciones: <ul style="list-style-type: none"> <li>• Usuario Logeado</li> <li>• Permisos Validados</li> </ul> |         |
| Post-Condiciones: <ul style="list-style-type: none"> <li>• Tareas creada</li> </ul>                                |         |
| Escenario Principal de Éxito                                                                                       |         |
| Actor                                                                                                              | Sistema |
| 1. Iniciar CU                                                                                                      |         |

|                                                   |                          |
|---------------------------------------------------|--------------------------|
|                                                   | 2. Mostrar Categorías    |
| 3. Seleccionar Categoría                          |                          |
|                                                   | 4. Mostrar Subcategorías |
| 4. Seleccionar Subcategoría                       |                          |
|                                                   | 5. Mostrar Tareas        |
| 6. Ingresar nueva tarea                           |                          |
| Repetir 6 hasta que el usuario lo desee           |                          |
| 7. Confirmar                                      |                          |
|                                                   | 8. Validar Confirmación  |
|                                                   | 9. Actualizar Tareas     |
|                                                   | 10. Fin CU               |
| Escenario de Alternativas                         |                          |
| 6.A Ingresar nueva tarea (Modificar Tareas)       |                          |
| Actor                                             | Sistema                  |
| 6.A.1 Seleccionar Tarea                           |                          |
| 6.A.2 Modificar datos de la Tarea                 |                          |
| Repetir 6.A.1-6.A.2 hasta que el usuario lo desee |                          |
|                                                   | 6.A.3 Volver al paso 6   |
| 6.B Ingresar nueva tarea (Eliminar Tareas)        |                          |
| Actor                                             | Sistema                  |

|                                                   |                          |
|---------------------------------------------------|--------------------------|
| 6.B.1 Seleccionar Tarea                           |                          |
| 6.B.2 Eliminar Tarea                              |                          |
| Repetir 6.B.1-6.B.2 hasta que el usuario lo desee |                          |
|                                                   | 6.B.3 Volver al paso 6   |
| 7.A Confirmar (Cancelar)                          |                          |
| Actor                                             | Sistema                  |
| 7.A.1 Cancelar Operación                          |                          |
|                                                   | 7.A.2 Cancelar Operación |
|                                                   | 7.A.3 Fin CU             |
| 7.B Confirmar (Modificar datos ingresados)        |                          |
| Actor                                             | Sistema                  |
|                                                   | 7.B.1 Volver al paso 5   |
|                                                   |                          |

Tabla 7.10-6

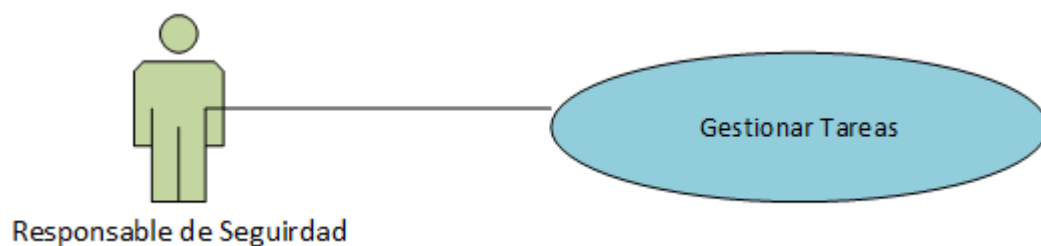


Ilustración 7.10-7

#### 7.10.3.7 Gestionar Incidente

|                             |
|-----------------------------|
| ID_CU: Gestionar Incidente  |
| Actor: Responsable de tarea |

|                                                                                                                                                                                       |                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Pre-Condiciones:                                                                                                                                                                      |                                                     |
| <ul style="list-style-type: none"> <li>• Usuario Logeado</li> <li>• Permisos Validados</li> <li>• Incidente Registrado</li> <li>• Estado del Incidente <i>"En proceso"</i></li> </ul> |                                                     |
| Post-Condiciones:                                                                                                                                                                     |                                                     |
| <ul style="list-style-type: none"> <li>• Tareas actualizadas</li> <li>• Incidente actualizado</li> </ul>                                                                              |                                                     |
| Escenario Principal de Éxito                                                                                                                                                          |                                                     |
| Actor                                                                                                                                                                                 | Sistema                                             |
| 1. Iniciar CU                                                                                                                                                                         |                                                     |
|                                                                                                                                                                                       | 2. Mostrar Incidentes en estado <i>"En Proceso"</i> |
| 3. Seleccionar Incidente                                                                                                                                                              |                                                     |
|                                                                                                                                                                                       | 4. Mostrar datos del Incidente                      |
|                                                                                                                                                                                       | 5. Mostrar tareas                                   |
| 6. Seleccionar Tarea                                                                                                                                                                  |                                                     |
| 7. Marcar Tarea como <i>"Completada"</i>                                                                                                                                              |                                                     |
| Repetir 6-7 hasta que el usuario lo desee                                                                                                                                             |                                                     |
| 8. Confirmar                                                                                                                                                                          |                                                     |
|                                                                                                                                                                                       | 9. Validar Confirmación                             |
|                                                                                                                                                                                       | 10. Actualizar Tareas                               |
|                                                                                                                                                                                       | 11. Fin CU                                          |
| Escenario de Alternativas                                                                                                                                                             |                                                     |
| 8.A Confirmar (Todas las Tareas completadas)                                                                                                                                          |                                                     |
| Actor                                                                                                                                                                                 | Sistema                                             |

|                                              |                                                       |
|----------------------------------------------|-------------------------------------------------------|
|                                              | 8.A.1 Solicitar descripción del Incidente             |
| 8.A.2 Ingresar descripción del Incidente     |                                                       |
| 8.A.3 Confirmar                              |                                                       |
|                                              | 8.A.4 Validar confirmación                            |
|                                              | 8.A.5 Actualizar Estado del Incidente a "Solucionado" |
|                                              | 8.A.6 Ir al paso 10                                   |
| 8.B Confirmar (Cancelar)                     |                                                       |
| Actor                                        | Sistema                                               |
| 8.B.1 Cancelar Operación                     |                                                       |
|                                              | 8.B.2 Cancelar Operación                              |
|                                              | 8.B.3 Volver al paso 2                                |
| 8.C Confirmar (Modificar Tareas completadas) |                                                       |
| Actor                                        | Sistema                                               |
|                                              | 8.C.1 Volver al paso 5                                |
| 8.A.3 Confirmar (Cancelar)                   |                                                       |
| Actor                                        | Sistema                                               |
| 8.A.3.1 Cancelar Operación                   |                                                       |
|                                              | 8.A.3.2 Cancelar Operación                            |
|                                              | 8.A.3.3 Volver al paso 2                              |

Tabla 7.10-7

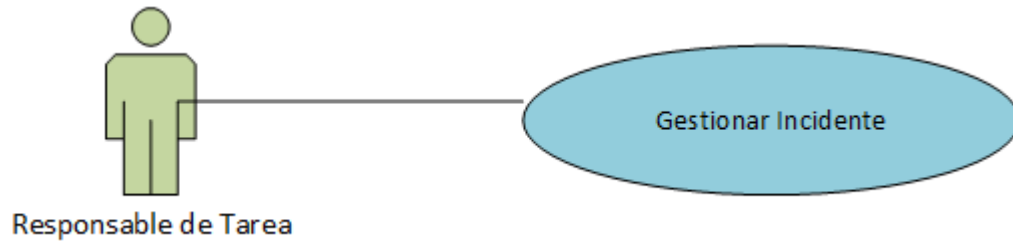


Ilustración 7.10-8

#### 7.10.3.8 Cargar Documentación de Seguridad

| ID_CU: Cargar Documentación de Seguridad                                                                              |                                               |
|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| Actor: Responsable de Seguridad de la Información                                                                     |                                               |
| Pre-Condiciones: <ul style="list-style-type: none"> <li>• Usuario Logeado</li> <li>• Permisos Validados</li> </ul>    |                                               |
| Post-Condiciones: <ul style="list-style-type: none"> <li>• Documento de Seguridad disponible para descarga</li> </ul> |                                               |
| Escenario Principal de Éxito                                                                                          |                                               |
| Actor                                                                                                                 | Sistema                                       |
| 1. Iniciar CU                                                                                                         |                                               |
|                                                                                                                       | 2. Mostrar listado de Documentos de Seguridad |
|                                                                                                                       | 3. Solicitar nuevo Documento de Seguridad     |
| 4. Cargar Documento                                                                                                   |                                               |
| 5. Confirmar                                                                                                          |                                               |
|                                                                                                                       | 6. Validar Confirmación                       |
|                                                                                                                       | 7. Actualizar listado de Documentos           |
|                                                                                                                       | 8. Fin CU                                     |
| Escenario de Alternativas                                                                                             |                                               |

| 5. Confirmar (Cancelar) |                        |
|-------------------------|------------------------|
| Actor                   | Sistema                |
| 5.1 Cancelar Operación  |                        |
|                         | 5.2 Cancelar Operación |
|                         | 5.3 Fin CU             |

Tabla 7.10-8

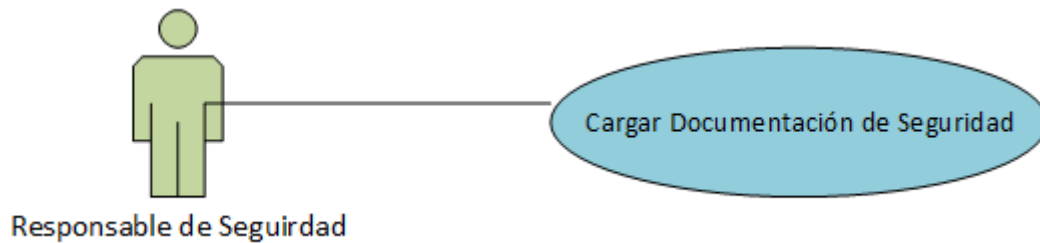


Ilustración 7.10-9

#### 7.10.3.9 Generar Informe de Incidentes registrados por Sub-Categoría

| ID_CU: Generar Informe de Incidentes registrados por Sub-Categoría                                                        |                              |
|---------------------------------------------------------------------------------------------------------------------------|------------------------------|
| Actor: Responsable de Seguridad de la Información                                                                         |                              |
| Pre-Condiciones: <ul style="list-style-type: none"> <li>• Usuario Logeado</li> <li>• Permisos Validados</li> </ul>        |                              |
| Post-Condiciones: <ul style="list-style-type: none"> <li>• Informe de Incidentes registrados por Sub-Categoría</li> </ul> |                              |
| Escenario Principal de Éxito                                                                                              |                              |
| Actor                                                                                                                     | Sistema                      |
| 1. Iniciar CU                                                                                                             |                              |
|                                                                                                                           | 2. Solicitar Rango de Fechas |
| 3. Ingresar Fecha de Inicio                                                                                               |                              |
| 4. Ingresar Fecha de Fin                                                                                                  |                              |

|                                                                                                                         |                                                                   |
|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 5. Confirmar                                                                                                            |                                                                   |
|                                                                                                                         | 6. Validar Fecha de Inicio ingresada                              |
|                                                                                                                         | 7. Validar Fecha de Fin ingresada                                 |
|                                                                                                                         | 8. Crear un auxiliar por cada Sub-Categoría                       |
|                                                                                                                         | 9. Buscar Incidente                                               |
|                                                                                                                         | 10. Incrementar auxiliar en base a la Sub-Categoría del Incidente |
| Repetir 9-10 para todos los Incidentes cuya fecha de ocurrencia se encuentre entre la Fecha de Inicio y la Fecha de Fin |                                                                   |
|                                                                                                                         | 11. Mostrar informe                                               |
|                                                                                                                         | 12. Fin CU                                                        |

#### Escenario de Alternativas

##### 5.A Confirmar (Cancelar)

| Actor                    | Sistema                  |
|--------------------------|--------------------------|
| 5.A.1 Cancelar Operación |                          |
|                          | 5.A.2 Cancelar Operación |
|                          | 5.A.3 Fin CU             |

##### 5.B Confirmar (Fecha de Inicio mal Ingresada)

| Actor                  | Sistema |
|------------------------|---------|
| 5.B.1 Volver al paso 3 |         |

##### 5.C Confirmar (Fecha de Fin mal Ingresada)

|                                                                      |                                              |
|----------------------------------------------------------------------|----------------------------------------------|
| Actor                                                                | Sistema                                      |
| 5.C.1 Volver al paso 4                                               |                                              |
| 6. Validar Fecha de Inicio ingresada (Fecha de Inicio mal Ingresada) |                                              |
| Actor                                                                | Sistema                                      |
|                                                                      | 6.1 Mostrar error "Fecha de Inicio Inválida" |
|                                                                      | 6.2 Volver al paso 3                         |
| 7. Validar Fecha de Fin ingresada (Fecha de Fin mal Ingresada)       |                                              |
| Actor                                                                | Sistema                                      |
|                                                                      | 7.1 Mostrar error "Fecha de Fin Inválida"    |
|                                                                      | 7.2 Volver al paso 4                         |

Tabla 7.10-9

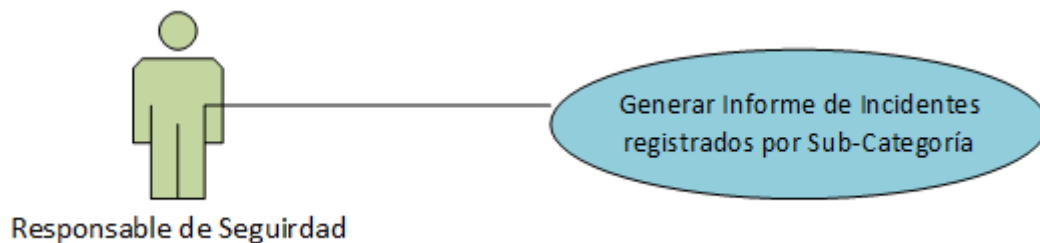


Ilustración 7.10-10

#### 7.10.3.10 Generar Informe de Incidentes registrados por Categoría

|                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------|
| ID_CU: Generar Informe de Incidentes registrados por Categoría                                                        |
| Actor: Responsable de Seguridad de la Información                                                                     |
| Pre-Condiciones: <ul style="list-style-type: none"> <li>• Usuario Logeado</li> <li>• Permisos Validados</li> </ul>    |
| Post-Condiciones: <ul style="list-style-type: none"> <li>• Informe de Incidentes registrados por Categoría</li> </ul> |

| Escenario Principal de Éxito                                                                                            |                                                               |
|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Actor                                                                                                                   | Sistema                                                       |
| 1. Iniciar CU                                                                                                           |                                                               |
|                                                                                                                         | 2. Solicitar Rango de Fechas                                  |
| 3. Ingresar Fecha de Inicio                                                                                             |                                                               |
| 4. Ingresar Fecha de Fin                                                                                                |                                                               |
| 5. Confirmar                                                                                                            |                                                               |
|                                                                                                                         | 6. Validar Fecha de Inicio ingresada                          |
|                                                                                                                         | 7. Validar Fecha de Fin ingresada                             |
|                                                                                                                         | 8. Crear un auxiliar por cada Categoría                       |
|                                                                                                                         | 9. Buscar Incidente                                           |
|                                                                                                                         | 10. Incrementar auxiliar en base a la Categoría del Incidente |
| Repetir 9-10 para todos los Incidentes cuya fecha de ocurrencia se encuentre entre la Fecha de Inicio y la Fecha de Fin |                                                               |
|                                                                                                                         | 11. Mostrar informe                                           |
|                                                                                                                         | 12. Fin CU                                                    |
| Escenario de Alternativas                                                                                               |                                                               |
| 5.A Confirmar (Cancelar)                                                                                                |                                                               |
| Actor                                                                                                                   | Sistema                                                       |
| 5.A.1 Cancelar Operación                                                                                                |                                                               |
|                                                                                                                         | 5.A.2 Cancelar Operación                                      |

|                                                                      |                                              |
|----------------------------------------------------------------------|----------------------------------------------|
|                                                                      | 5.A.3 Fin CU                                 |
| 5.B Confirmar (Fecha de Inicio mal Ingresada)                        |                                              |
| Actor                                                                | Sistema                                      |
| 5.B.1 Volver al paso 3                                               |                                              |
| 5.C Confirmar (Fecha de Fin mal Ingresada)                           |                                              |
| Actor                                                                | Sistema                                      |
| 5.C.1 Volver al paso 4                                               |                                              |
| 6. Validar Fecha de Inicio ingresada (Fecha de Inicio mal Ingresada) |                                              |
| Actor                                                                | Sistema                                      |
|                                                                      | 6.1 Mostrar error "Fecha de Inicio Inválida" |
|                                                                      | 6.2 Volver al paso 3                         |
| 7. Validar Fecha de Fin ingresada (Fecha de Fin mal Ingresada)       |                                              |
| Actor                                                                | Sistema                                      |
|                                                                      | 7.1 Mostrar error "Fecha de Fin Inválida"    |
|                                                                      | 7.2 Volver al paso 4                         |

Tabla 7.10-10

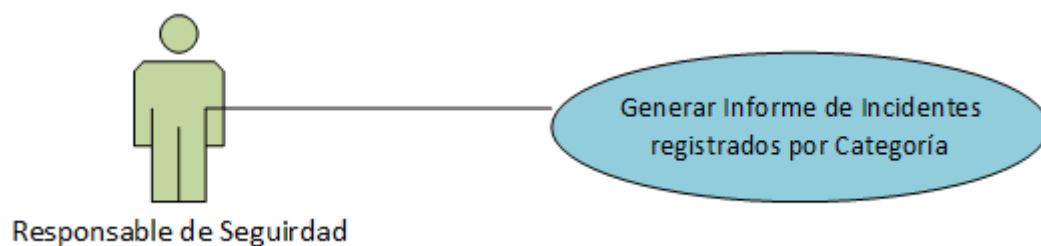


Ilustración 7.10-11

7.10.3.11 Generar Informe de Tiempo Total por Sub-Categoría de Incidente

|                                                                                                                              |                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| ID_CU: Generar Informe de Tiempo Total por Sub-Categoría de Incidente                                                        |                                                                                        |
| Actor: Responsable de Seguridad de la Información                                                                            |                                                                                        |
| Pre-Condiciones: <ul style="list-style-type: none"> <li>• Usuario Logeado</li> <li>• Permisos Validados</li> </ul>           |                                                                                        |
| Post-Condiciones: <ul style="list-style-type: none"> <li>• Informe de Tiempo Total por Sub-Categoría de Incidente</li> </ul> |                                                                                        |
| Escenario Principal de Éxito                                                                                                 |                                                                                        |
| Actor                                                                                                                        | Sistema                                                                                |
| 1. Iniciar CU                                                                                                                |                                                                                        |
|                                                                                                                              | 2. Solicitar Rango de Fechas                                                           |
| 3. Ingresar Fecha de Inicio                                                                                                  |                                                                                        |
| 4. Ingresar Fecha de Fin                                                                                                     |                                                                                        |
| 5. Confirmar                                                                                                                 |                                                                                        |
|                                                                                                                              | 6. Validar Fecha de Inicio ingresada                                                   |
|                                                                                                                              | 7. Validar Fecha de Fin ingresada                                                      |
|                                                                                                                              | 8. Crear un auxiliar por cada Sub-Categoría                                            |
|                                                                                                                              | 9. Buscar Incidente                                                                    |
|                                                                                                                              | 10. Calcular tiempo de resolución de Incidente                                         |
|                                                                                                                              | 11. Acumular tiempo de resolución en auxiliar en base a la Sub-Categoría del Incidente |
| Repetir 9-11 para todos los Incidentes cuya fecha de ocurrencia se encuentre entre la Fecha de Inicio y la Fecha de Fin      |                                                                                        |

|                                                                      |                                              |
|----------------------------------------------------------------------|----------------------------------------------|
|                                                                      | 12. Mostrar informe                          |
|                                                                      | 13. Fin CU                                   |
| Escenario de Alternativas                                            |                                              |
| 5.A Confirmar (Cancelar)                                             |                                              |
| Actor                                                                | Sistema                                      |
| 5.A.1 Cancelar Operación                                             |                                              |
|                                                                      | 5.A.2 Cancelar Operación                     |
|                                                                      | 5.A.3 Fin CU                                 |
| 5.B Confirmar (Fecha de Inicio mal Ingresada)                        |                                              |
| Actor                                                                | Sistema                                      |
| 5.B.1 Volver al paso 3                                               |                                              |
| 5.C Confirmar (Fecha de Fin mal Ingresada)                           |                                              |
| Actor                                                                | Sistema                                      |
| 5.C.1 Volver al paso 4                                               |                                              |
| 6. Validar Fecha de Inicio ingresada (Fecha de Inicio mal Ingresada) |                                              |
| Actor                                                                | Sistema                                      |
|                                                                      | 6.1 Mostrar error "Fecha de Inicio Inválida" |
|                                                                      | 6.2 Volver al paso 3                         |
| 7. Validar Fecha de Fin ingresada (Fecha de Fin mal Ingresada)       |                                              |

|       |                                           |
|-------|-------------------------------------------|
| Actor | Sistema                                   |
|       | 7.1 Mostrar error “Fecha de Fin Inválida” |
|       | 7.2 Volver al paso 4                      |

Tabla 7.10-11

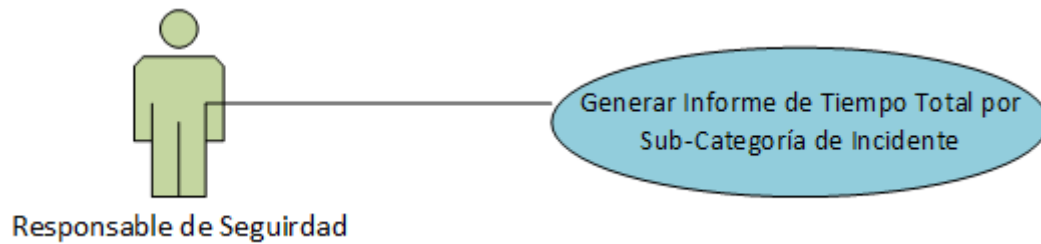


Ilustración 7.10-12

#### 7.10.3.12 Generar Informe de Tiempo Promedio por Sub-Categoría de Incidente

|                                                                                                                              |                              |
|------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| ID_CU: Generar Informe de Tiempo Promedio por Sub-Categoría de Incidente                                                     |                              |
| Actor: Responsable de Seguridad de la Información                                                                            |                              |
| Pre-Condiciones: <ul style="list-style-type: none"> <li>• Usuario Logeado</li> <li>• Permisos Validados</li> </ul>           |                              |
| Post-Condiciones: <ul style="list-style-type: none"> <li>• Informe de Tiempo Total por Sub-Categoría de Incidente</li> </ul> |                              |
| Escenario Principal de Éxito                                                                                                 |                              |
| Actor                                                                                                                        | Sistema                      |
| 1. Iniciar CU                                                                                                                |                              |
|                                                                                                                              | 2. Solicitar Rango de Fechas |
| 3. Ingresar Fecha de Inicio                                                                                                  |                              |
| 4. Ingresar Fecha de Fin                                                                                                     |                              |
| 5. Confirmar                                                                                                                 |                              |

|                                                                                                                          |                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
|                                                                                                                          | 6. Validar Fecha de Inicio ingresada                                                   |
|                                                                                                                          | 7. Validar Fecha de Fin ingresada                                                      |
|                                                                                                                          | 8. Crear un auxiliar por cada Sub-Categoría, para acumular tiempos de resolución       |
|                                                                                                                          | 9. Crear un auxiliar por cada Sub-Categoría para acumular cantidad de Incidentes       |
|                                                                                                                          | 10. Buscar Incidente                                                                   |
|                                                                                                                          | 11. Calcular tiempo de resolución de Incidente                                         |
|                                                                                                                          | 12. Acumular tiempo de resolución en auxiliar en base a la Sub-Categoría del Incidente |
|                                                                                                                          | 13. Incrementar auxiliar correspondiente a la Sub-Categoría del Incidente              |
| Repetir 10-13 para todos los Incidentes cuya fecha de ocurrencia se encuentre entre la Fecha de Inicio y la Fecha de Fin |                                                                                        |
|                                                                                                                          | 14. Calcular promedios de tiempo de resolución por Sub-Categoría                       |
|                                                                                                                          | 12. Mostrar informe                                                                    |
|                                                                                                                          | 13. Fin CU                                                                             |

#### Escenario de Alternativas

##### 5.A Confirmar (Cancelar)

| Actor                    | Sistema                  |
|--------------------------|--------------------------|
| 5.A.1 Cancelar Operación |                          |
|                          | 5.A.2 Cancelar Operación |
|                          | 5.A.3 Fin CU             |

|                                                                      |                                              |
|----------------------------------------------------------------------|----------------------------------------------|
| 5.B Confirmar (Fecha de Inicio mal Ingresada)                        |                                              |
| Actor                                                                | Sistema                                      |
| 5.B.1 Volver al paso 3                                               |                                              |
| 5.C Confirmar (Fecha de Fin mal Ingresada)                           |                                              |
| Actor                                                                | Sistema                                      |
| 5.C.1 Volver al paso 4                                               |                                              |
| 6. Validar Fecha de Inicio ingresada (Fecha de Inicio mal Ingresada) |                                              |
| Actor                                                                | Sistema                                      |
|                                                                      | 6.1 Mostrar error "Fecha de Inicio Inválida" |
|                                                                      | 6.2 Volver al paso 3                         |
| 7. Validar Fecha de Fin ingresada (Fecha de Fin mal Ingresada)       |                                              |
| Actor                                                                | Sistema                                      |
|                                                                      | 7.1 Mostrar error "Fecha de Fin Inválida"    |
|                                                                      | 7.2 Volver al paso 4                         |

Tabla 7.10-12

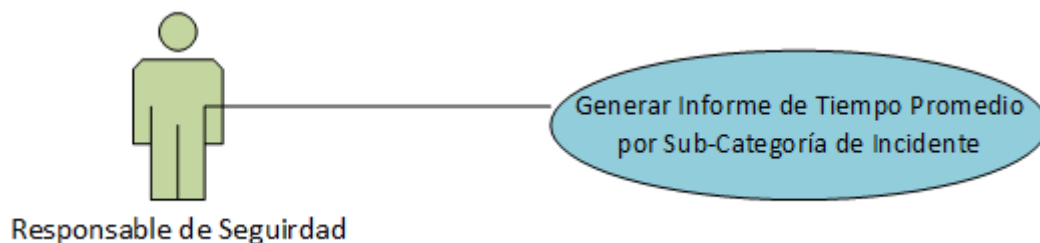
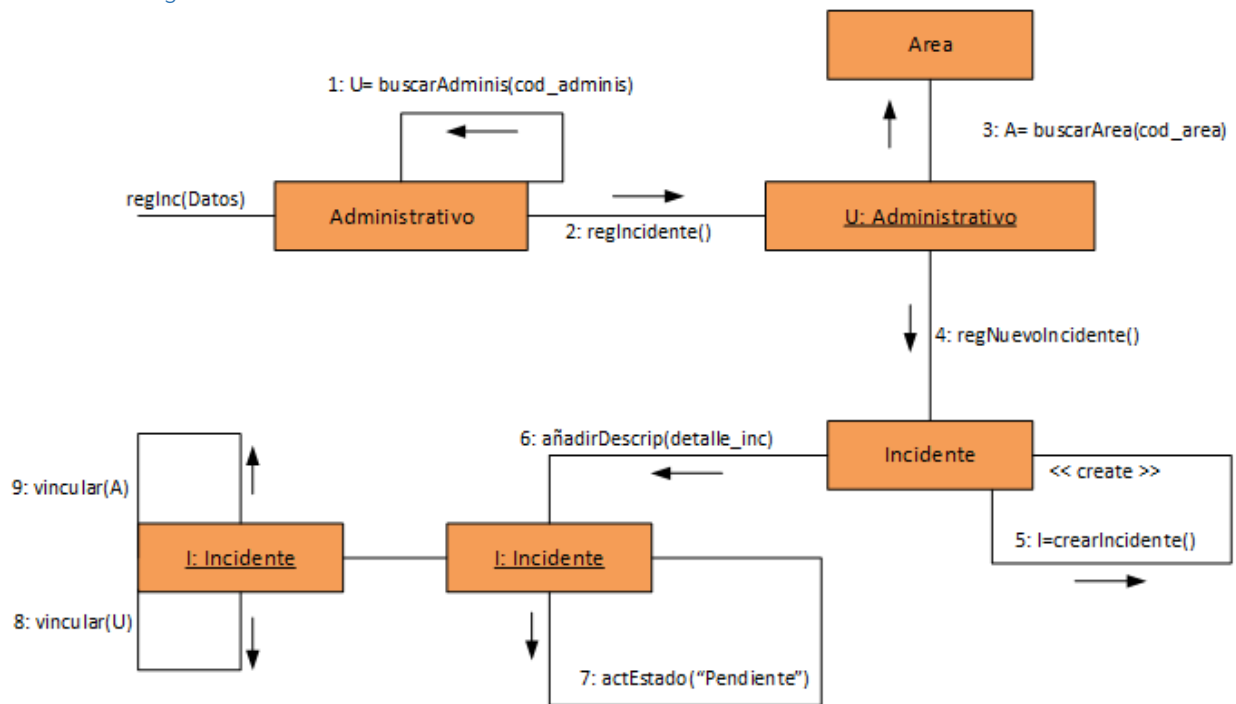


Ilustración 7.10-13

#### 7.10.4 Diagramas de colaboración

##### 7.10.4.1 Registrar Incidente



Datos= cod\_adminis + cod\_area + detalle\_inc

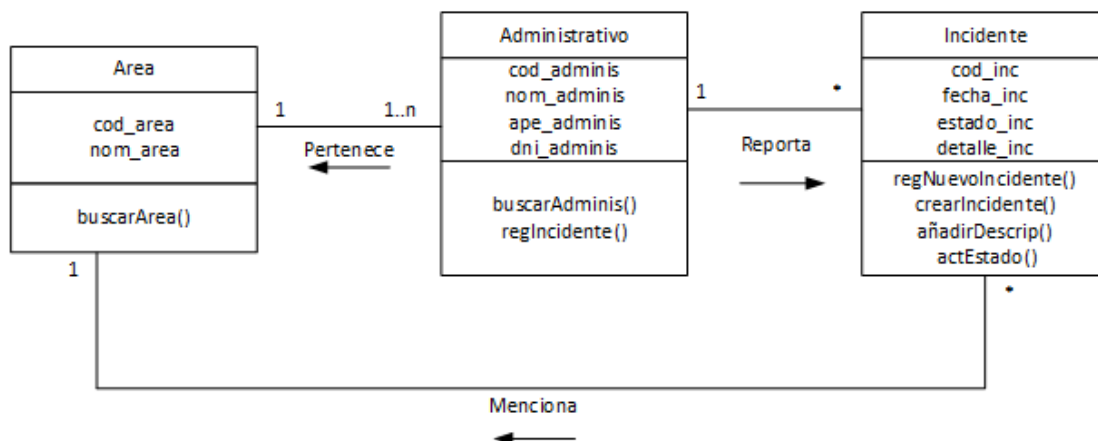
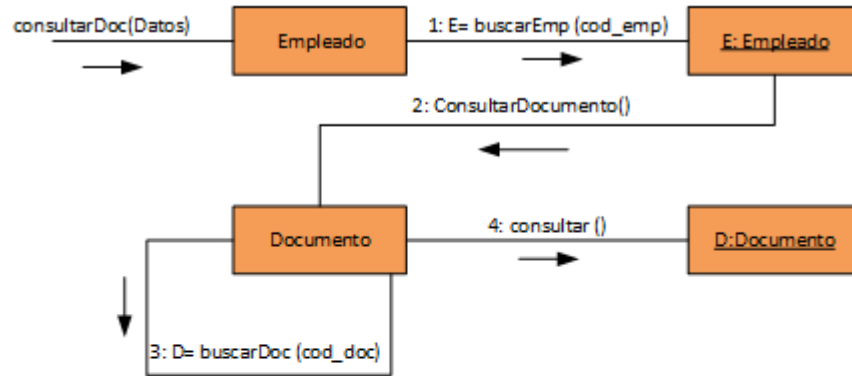


Ilustración 7.10-14

#### 7.10.4.2 Visualizar documentación de Seguridad



Datos= cod\_emp + cod\_doc

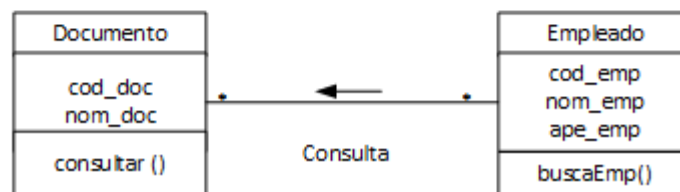
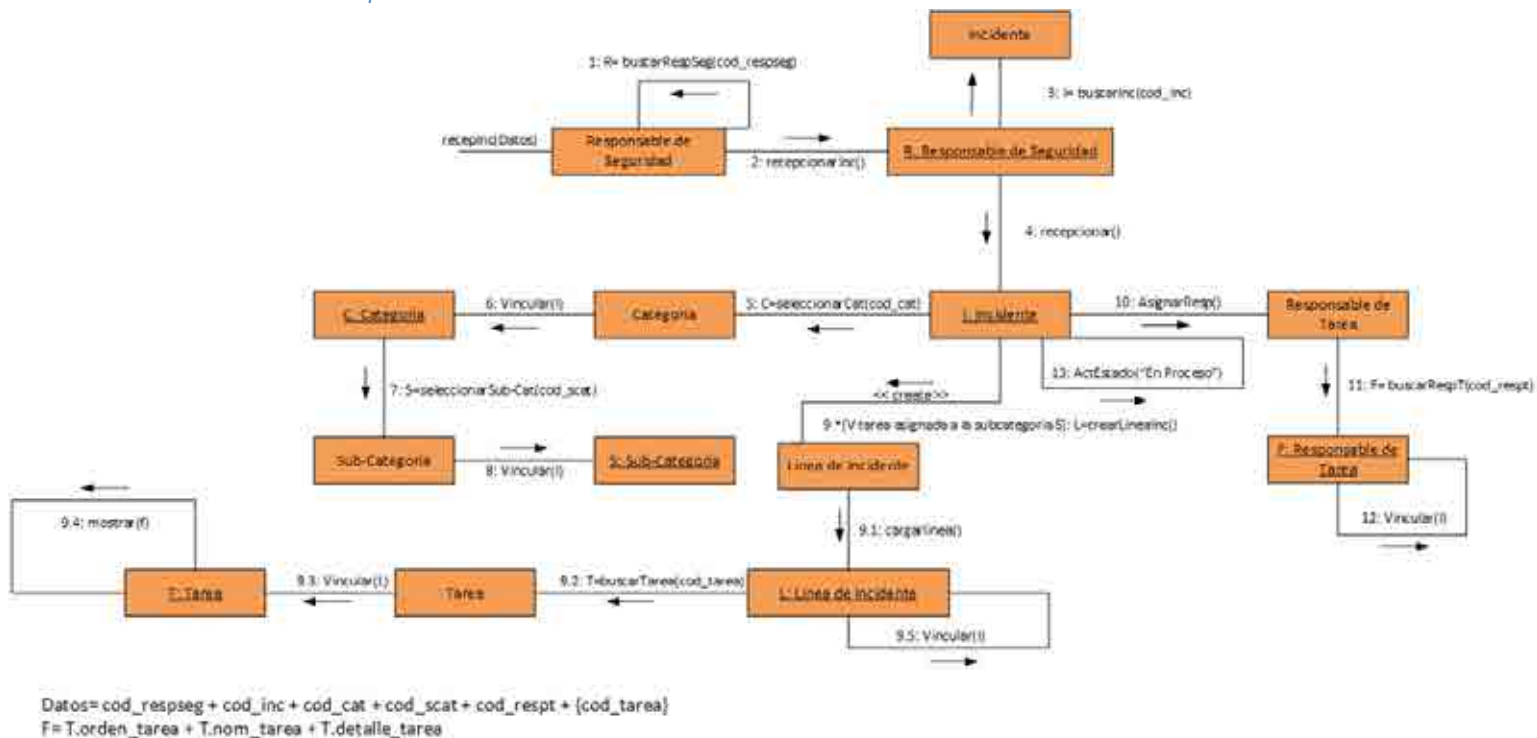


Ilustración 7.10-15

#### 7.10.4.3 Recepcionar Incidente



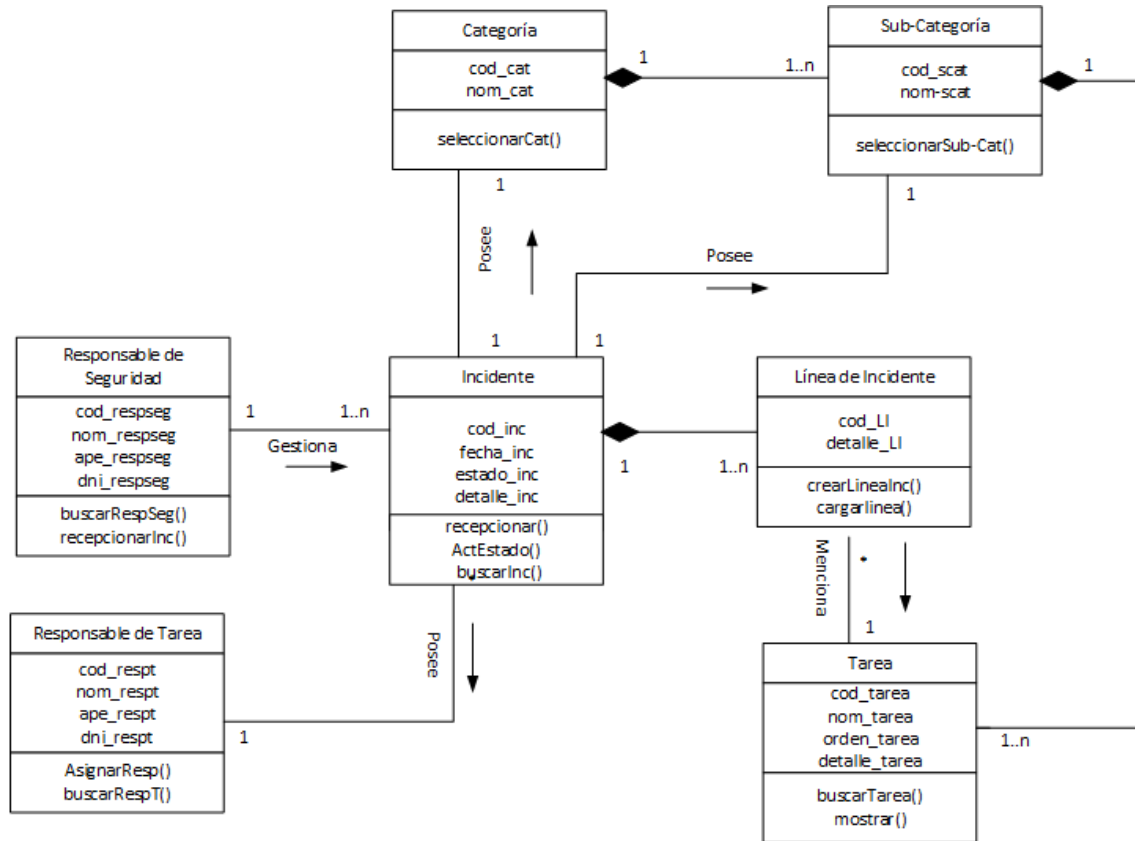
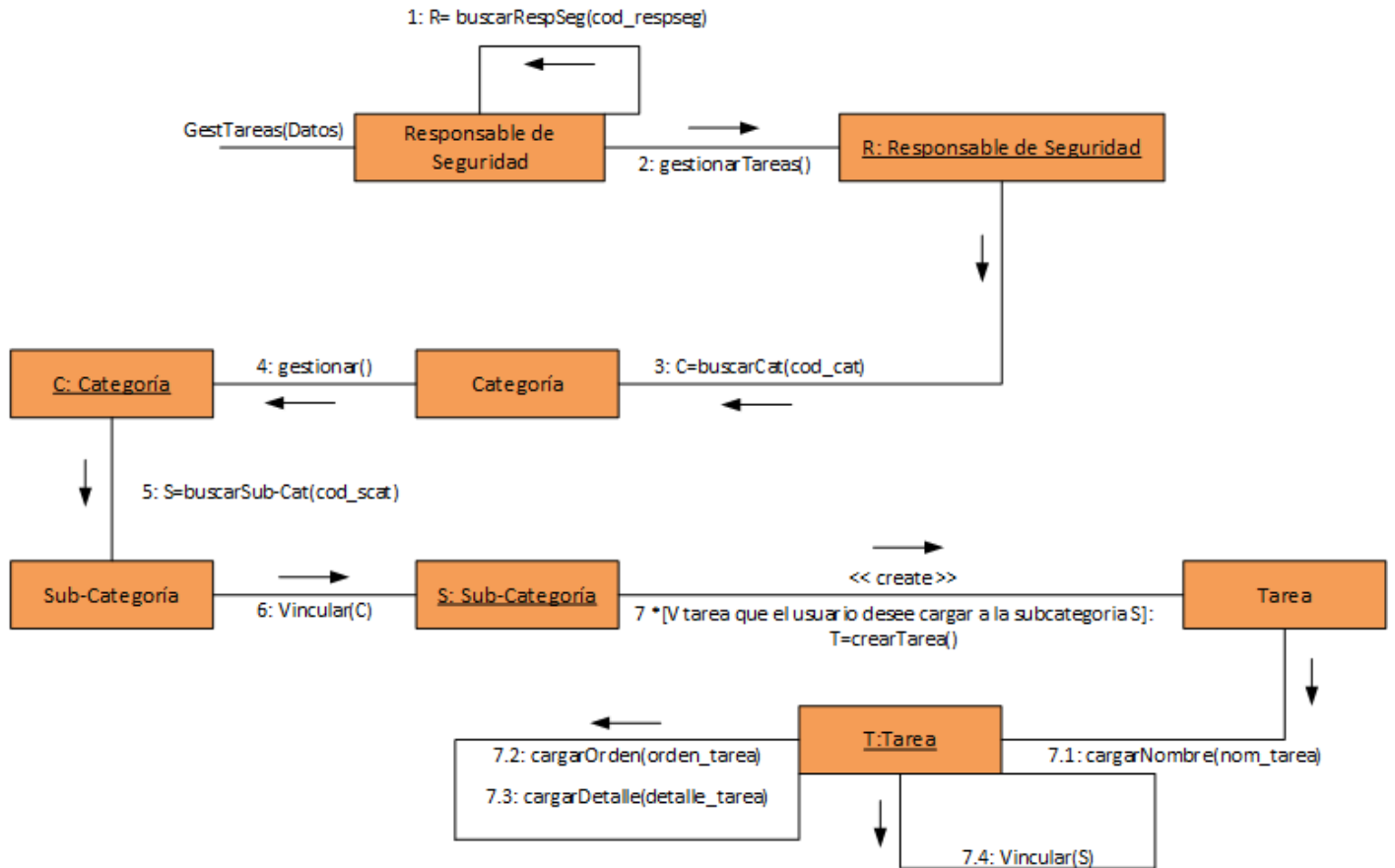


Ilustración 7.10-16



Datos= cod\_respseg + cod\_cat + cod\_scat + {nom\_tarea + detalle\_tarea + orden\_tarea}

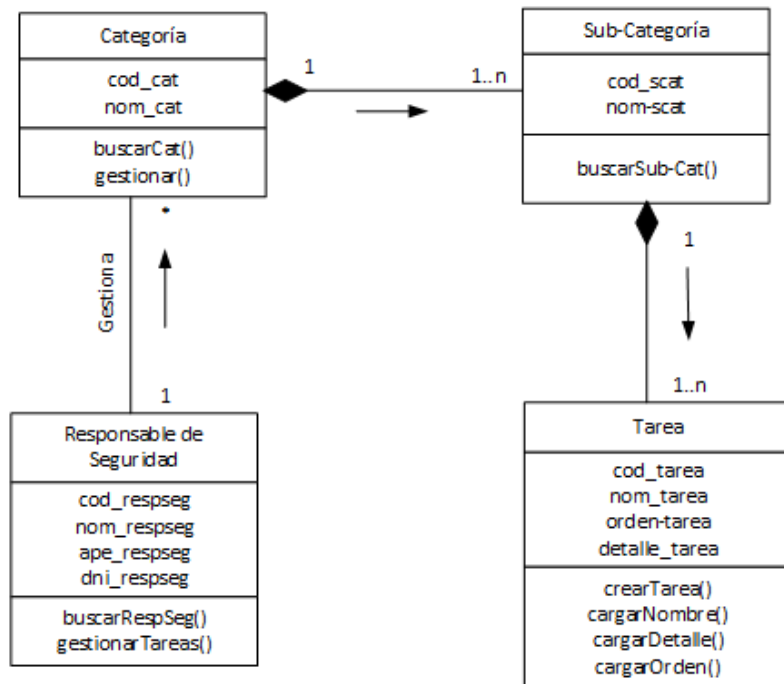
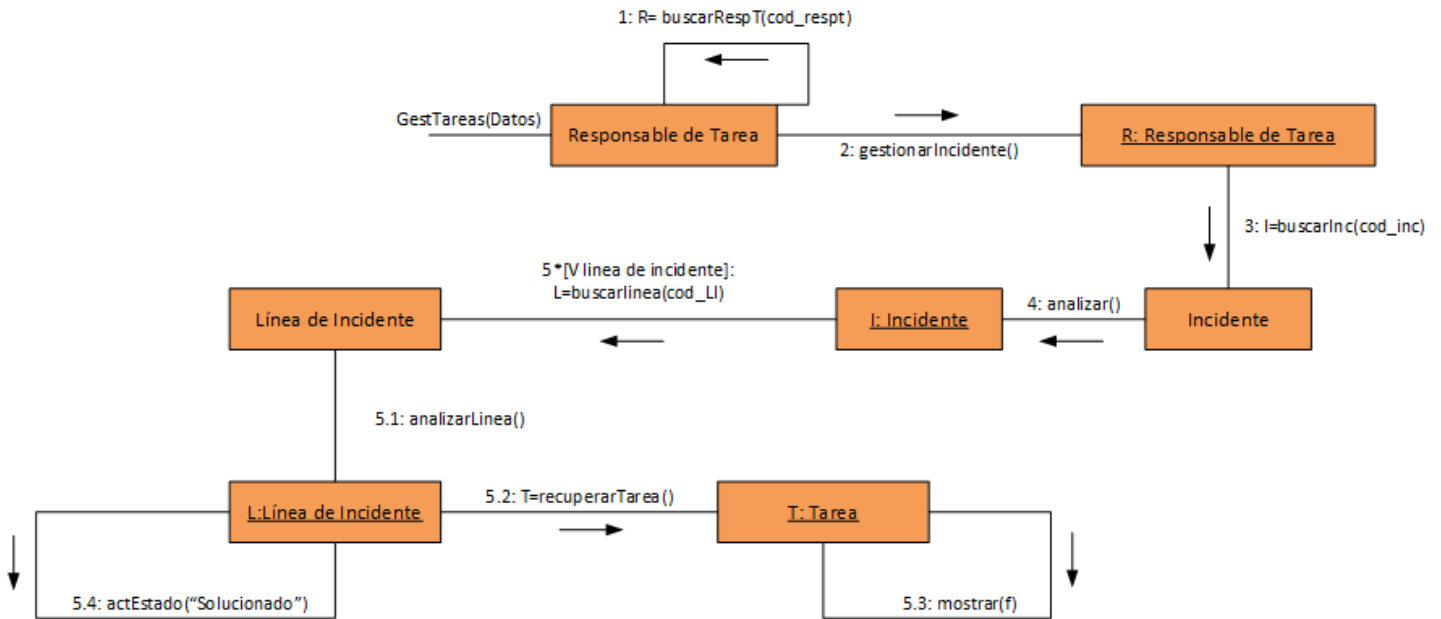


Ilustración 7.10-17



Datos= cod\_respt + cod\_inc + cod\_LI  
 F= T.orden\_tarea + T.nom\_tarea + T.detalle\_tarea

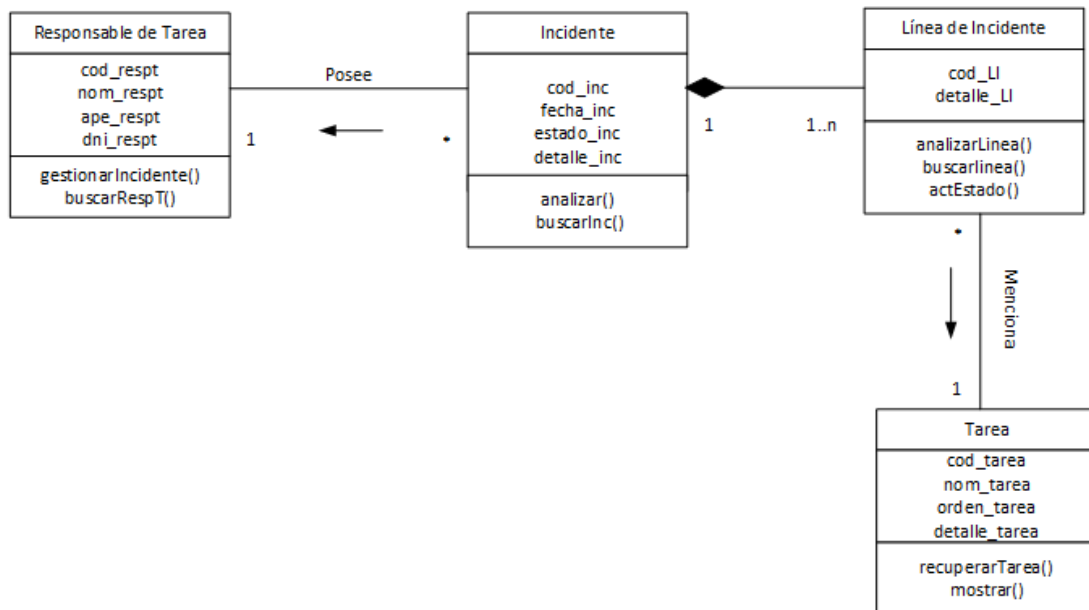


Ilustración 7.10-18

7.10.4.6 Cargar Documentación de Seguridad

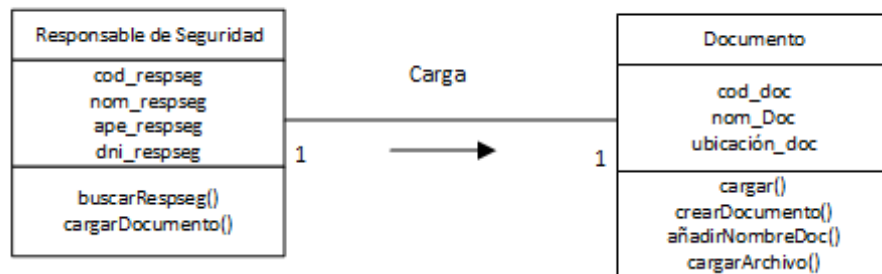
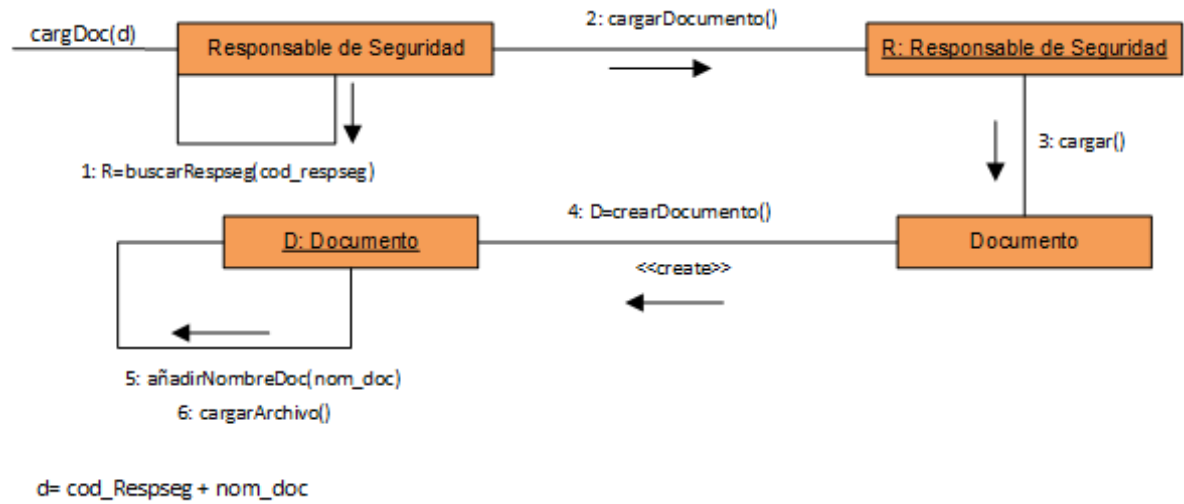


Ilustración 7.10-19

7.10.4.7 Generar Informe de Incidentes registrados por Sub-Categoría

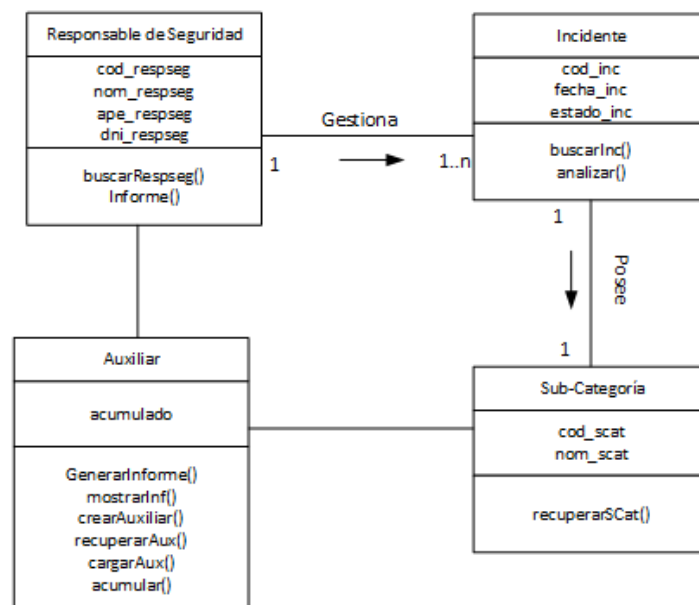
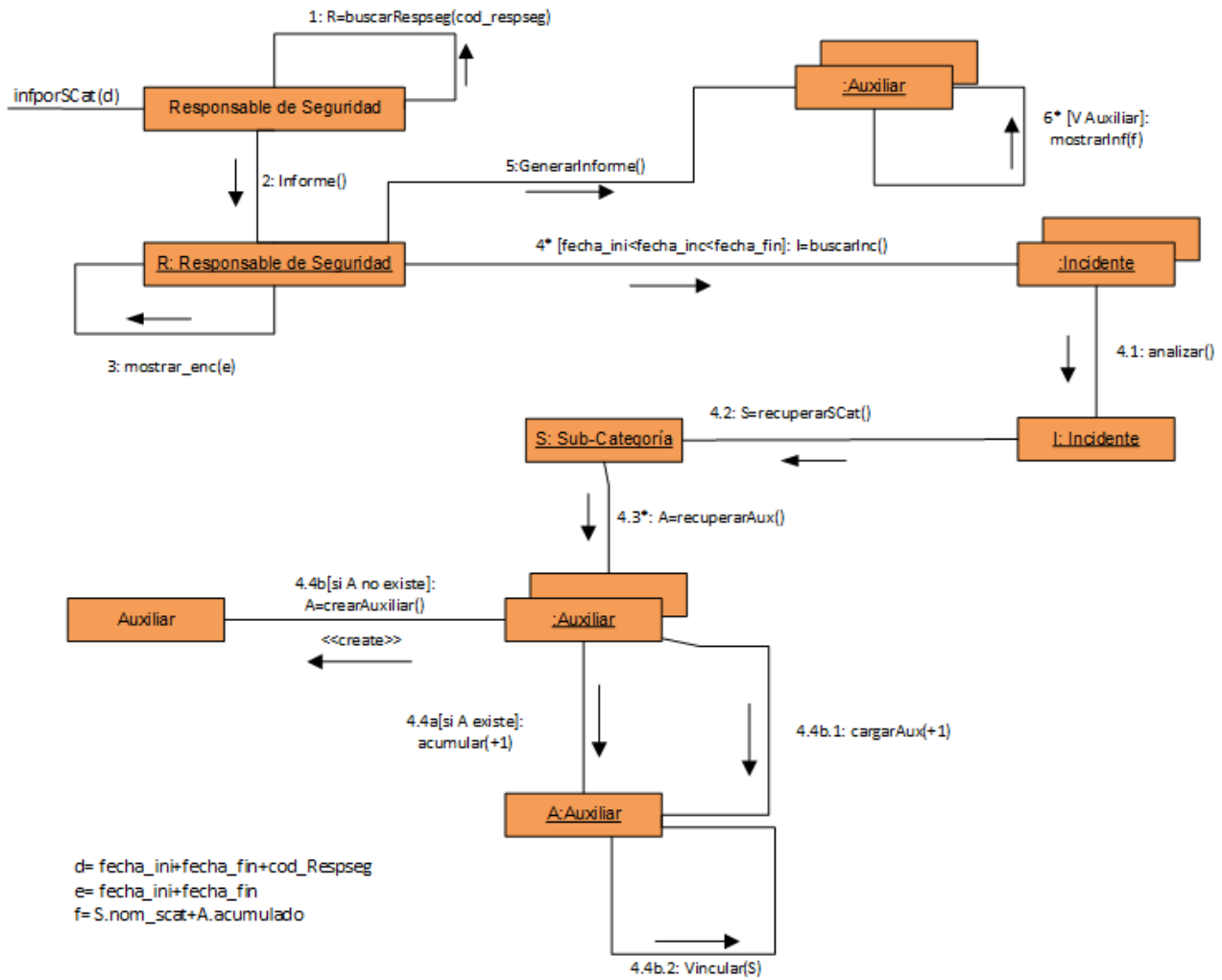


Ilustración 7.10-20

7.10.4.8 Generar Informe de Incidentes registrados por Categoría

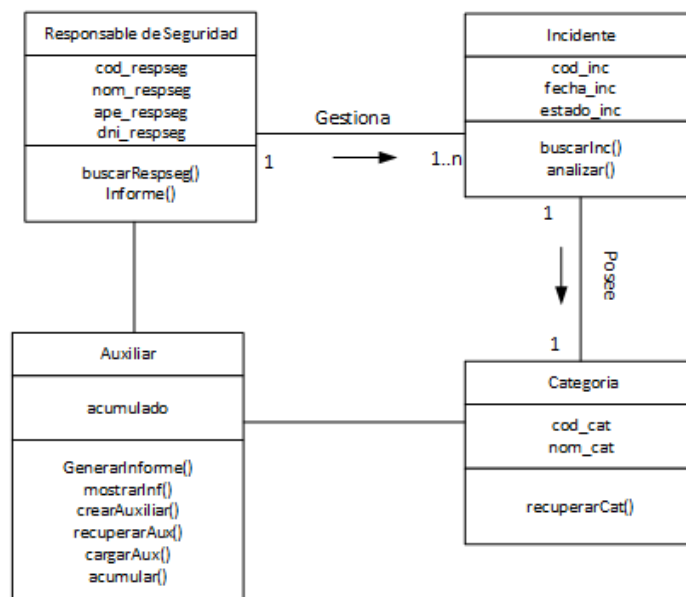
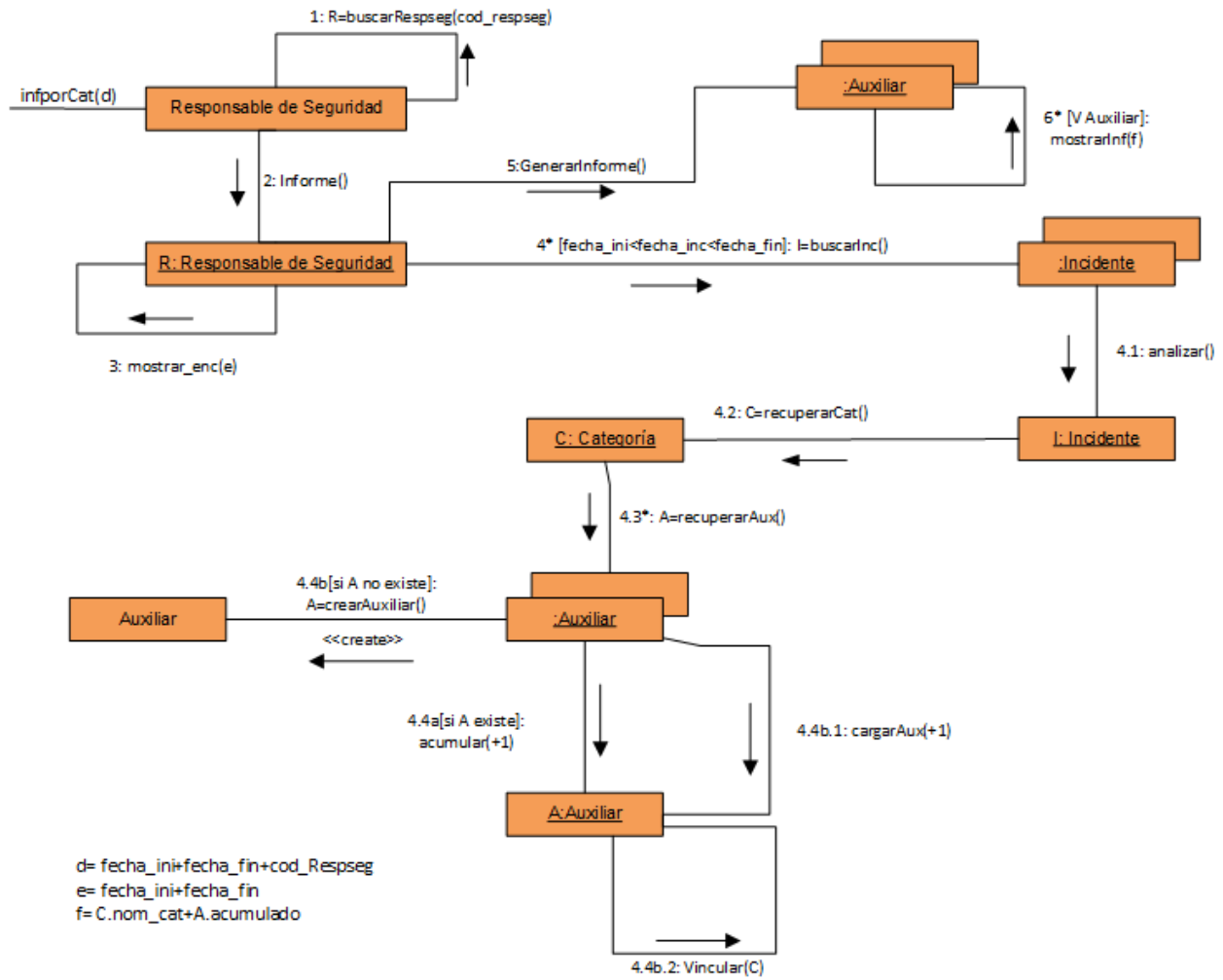


Ilustración 7.10-21

7.10.4.9 Generar Informe de Tiempo Total por Sub-Categoría de Incidente

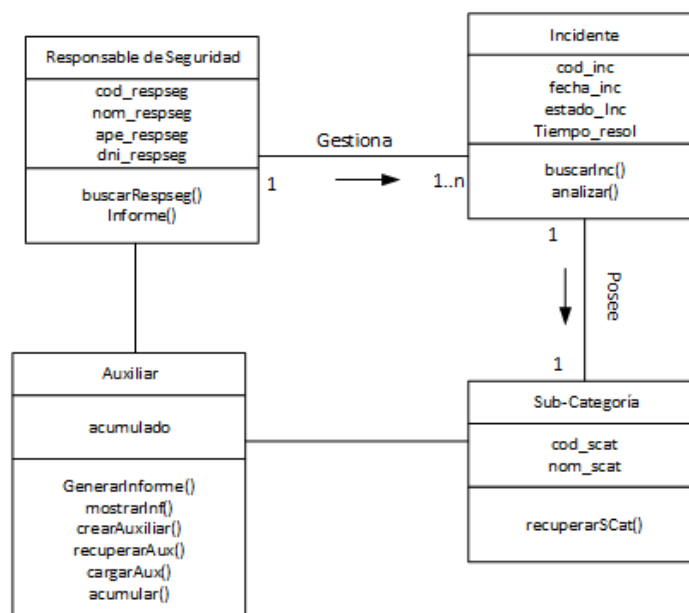
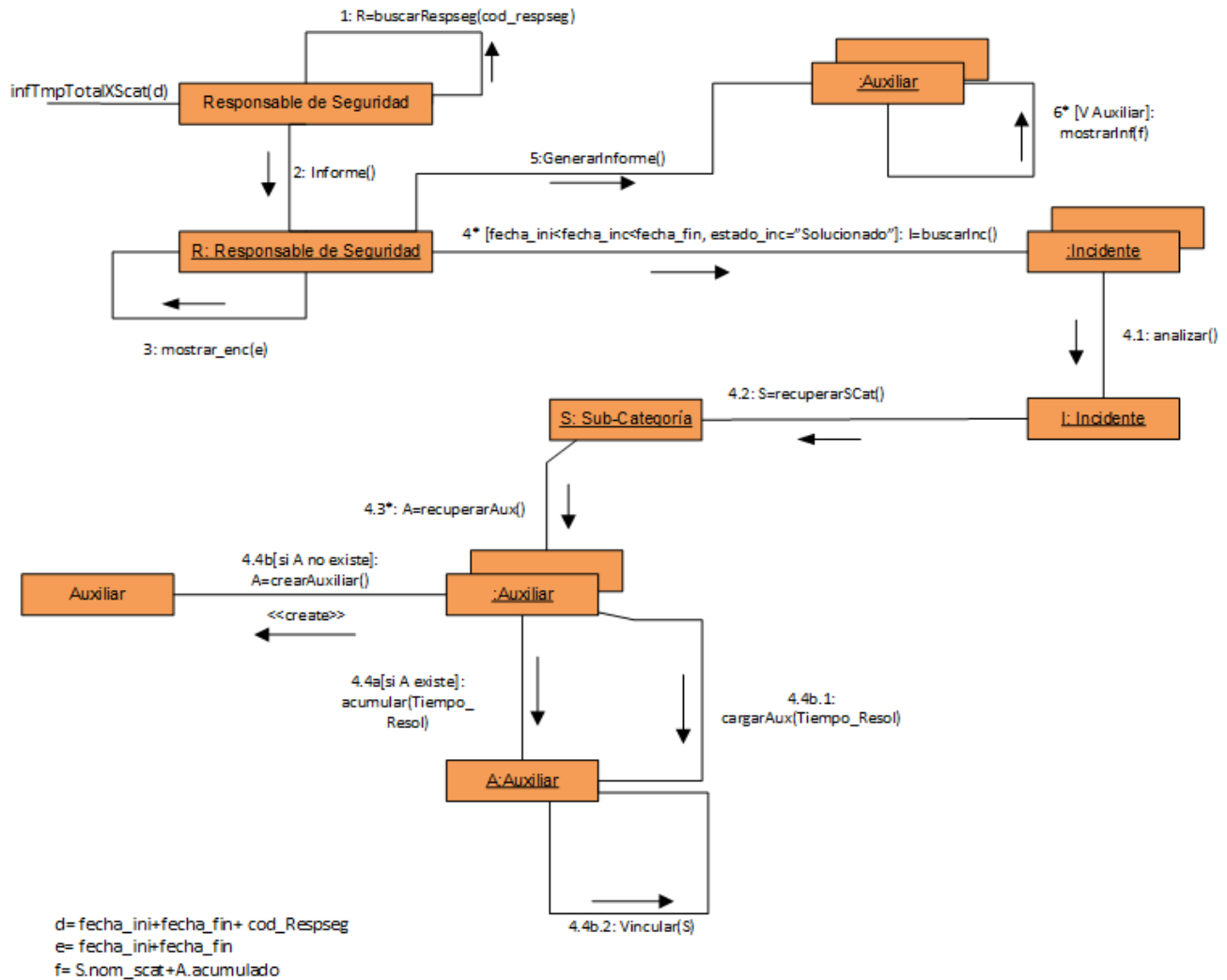


Ilustración 7.10-22

7.10.4.10 Generar Informe de Tiempo Promedio por Sub-Categoría de Incidente

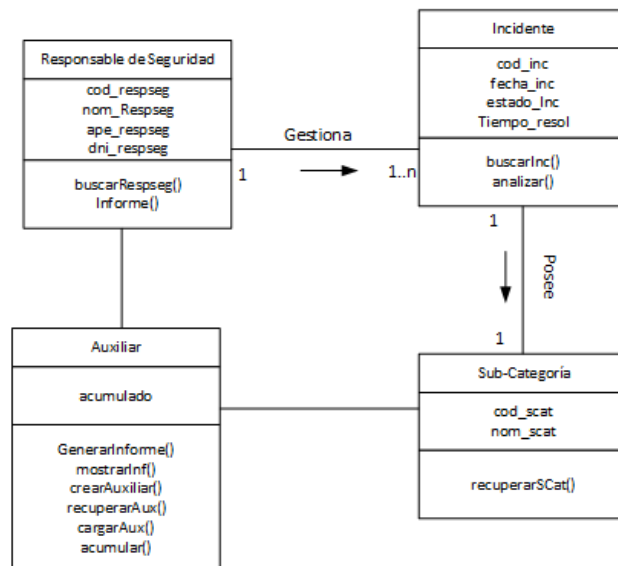
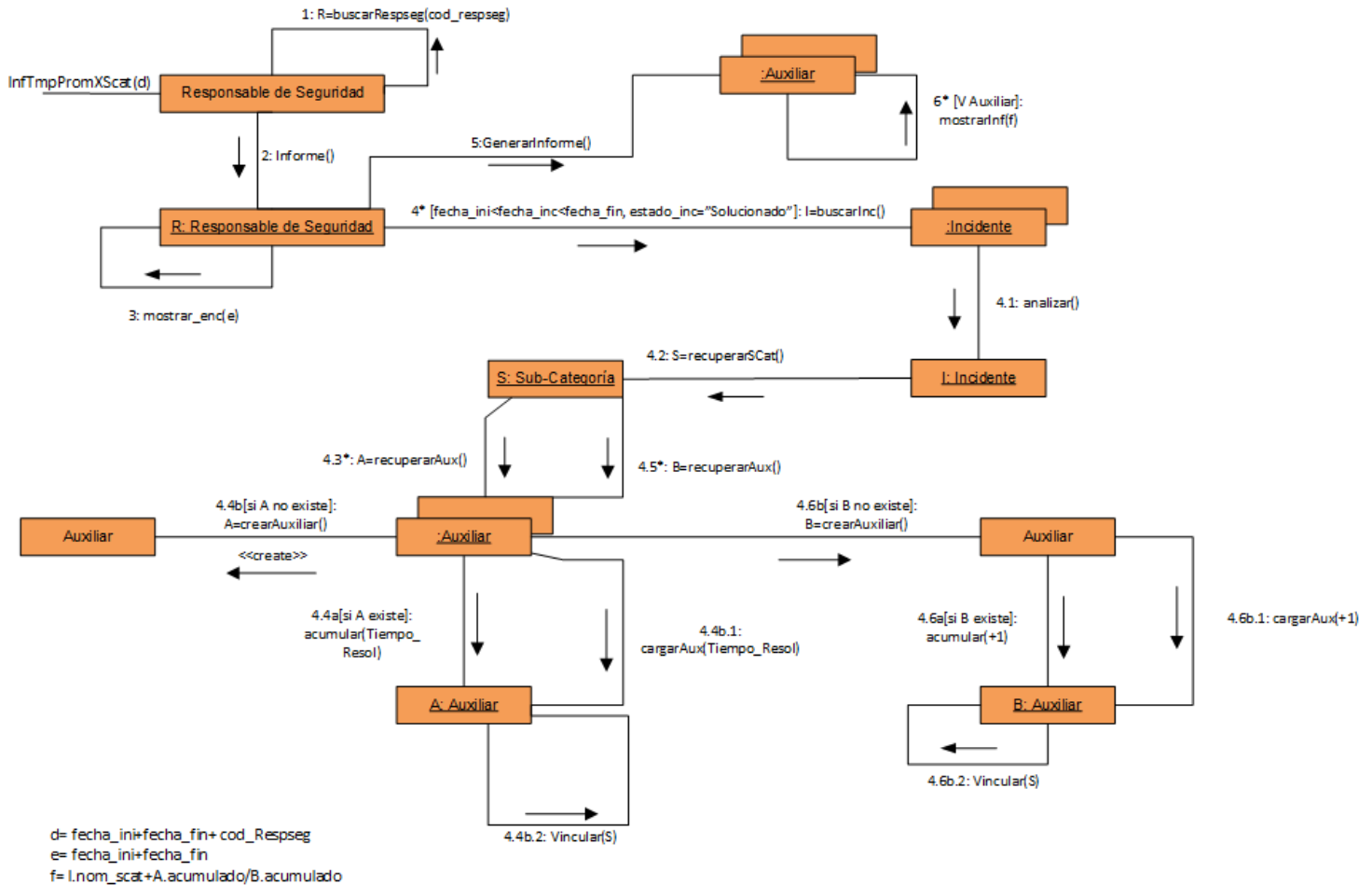


Ilustración 7.10-23

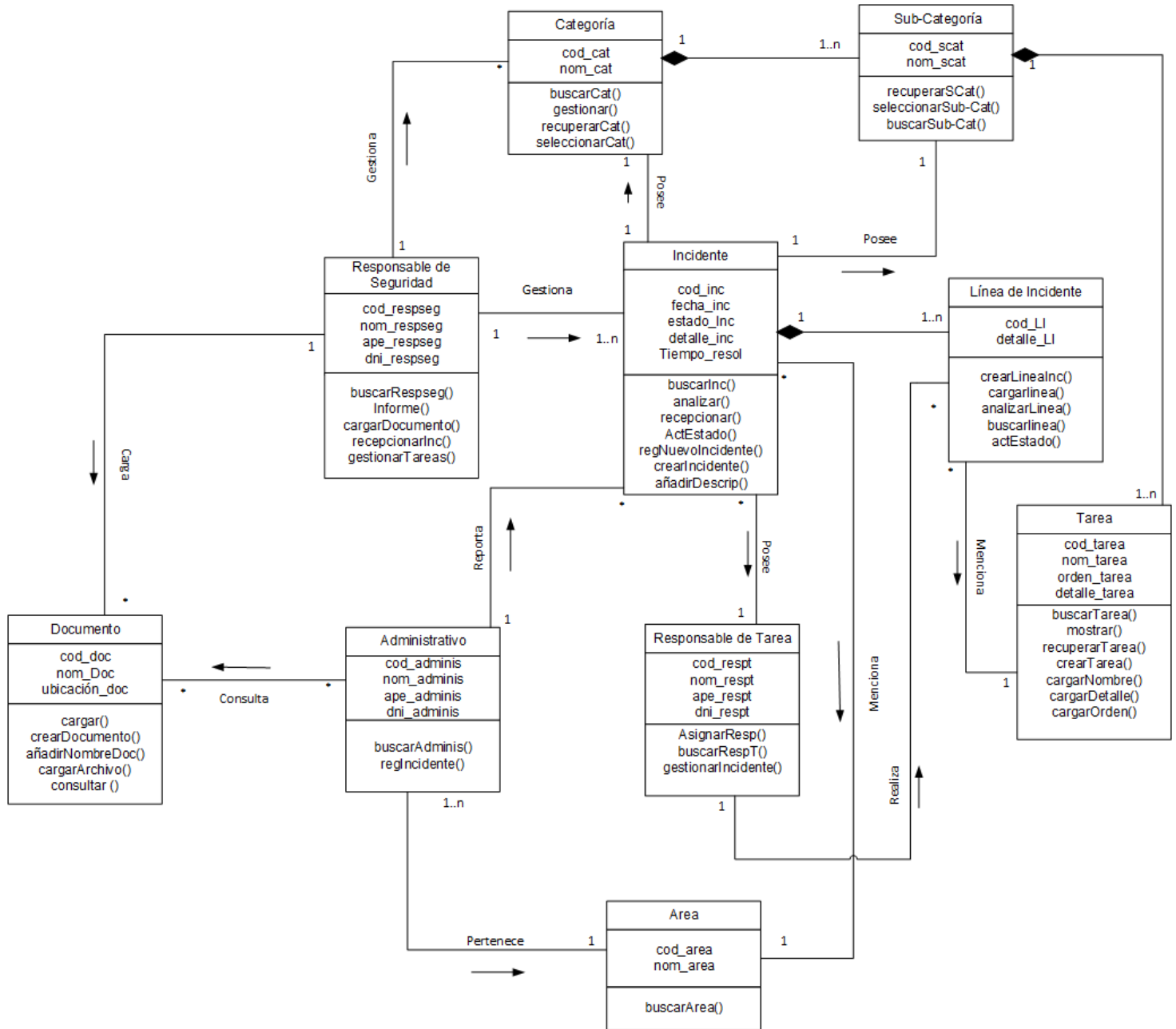


Ilustración 7.10-24

#### 7.10.6 Vistazo General del Prototipo

A continuación, se detalla el funcionamiento del Prototipo desarrollado.

##### Acciones del Usuario (Administrativo que reporta los incidentes.)

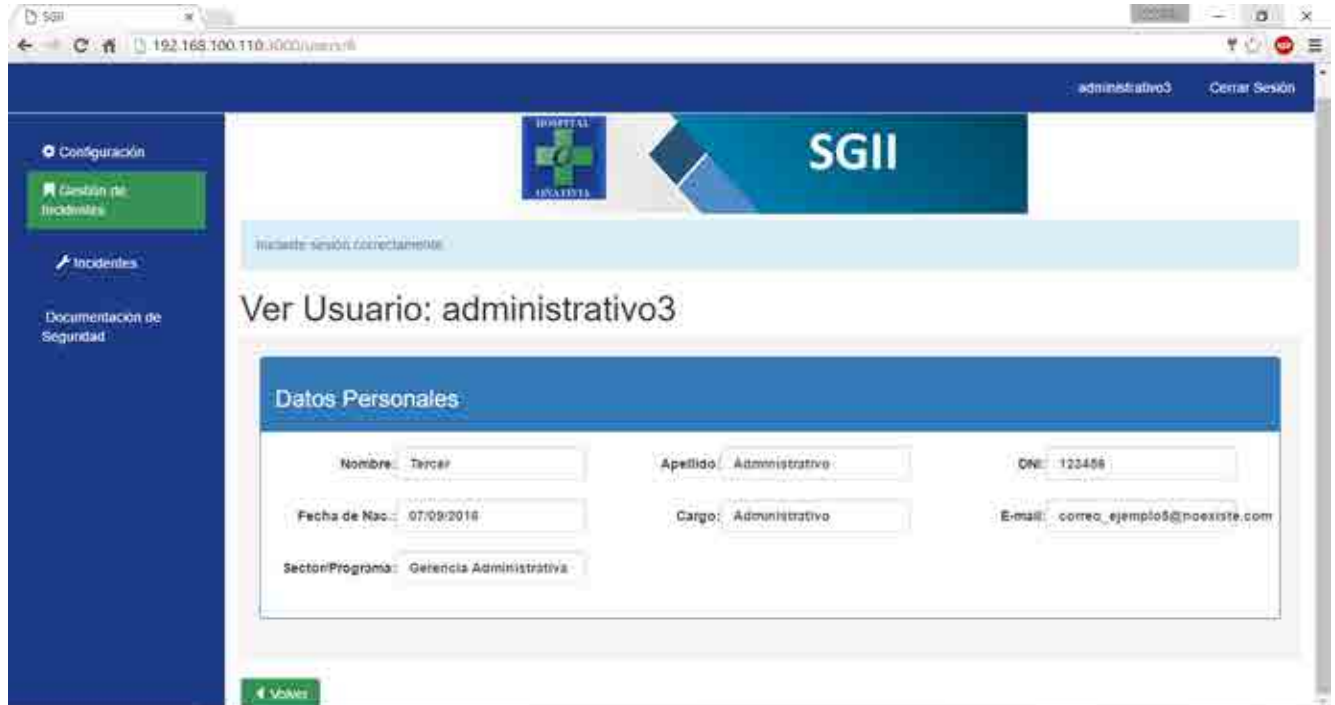


Ilustración 7.10-25

La imagen anterior corresponde a la pantalla de inicio de un usuario común. Como podemos ver, en la parte lateral izquierda, se ofrece al usuario un menú con las diferentes características disponibles para el mismo.

Si el usuario hace clic en “Incidentes” (Menú lateral izquierdo), la siguiente pantalla le aparecerá.



Ilustración 7.10-26

Podemos observar que al usuario se le muestra:

- Un buscador (botón buscar): haciendo uso de los diferentes filtros, es posible buscar los incidentes que este haya registrado en el sistema. Si el usuario desea buscar un incidente en particular, solo deberá completar algún dato del filtro para así obtener información sobre este incidente.
- Cargar Incidente (botón superior derecho): es posible para el usuario cargar/reportar a través del sistema incidentes de seguridad de la información.

Si el usuario desea cargar un incidente, debe hacer clic en Cargar Incidente (botón superior derecho), y la siguiente pantalla le será mostrada.

The screenshot shows a web browser window displaying a form titled 'Registrar Incidente'. The form is part of a system with a blue sidebar containing links for 'Configuración', 'Gestión de Incidentes', and 'Documentación de Seguridad'. The form itself has a header 'Datos Generales:' and contains several input fields: 'Fecha:' (07/09/2016 14:53), 'Reportado por:' (administrativo3), 'Sector/Programa:' (Gerencia Administrativa), 'Descripción del incidente:', 'Título descriptivo:' (Virus en computadora), and 'Descripción del problema:' (Amenaza detectada por antivirus. Mal funcionamiento del equipo (Esta tarde)). There are 'Guardar' buttons at the bottom right of the form sections.

Ilustración 7.10-27

Como puede observarse en la anterior imagen, el reporte del incidente cuenta con un encabezado en donde se detalla la fecha del reporte, la persona que realiza el mismo (usuario) y el sector/programa al cual pertenece. Cuenta además con una descripción del incidente, en donde el usuario debe indicar un título descriptivo del mismo y también debe brindar una pequeña descripción del problema. Cuando el usuario hace clic en guardar, el reporte es registrado por el sistema (en estado “pendiente”) y al mismo tiempo, el sistema avisa a través de un mail al administrador del sistema (responsable de seguridad) de la existencia de un nuevo incidente que debe ser atendido. A continuación se muestra el mail de aviso que es recibido en el correo electrónico del administrador del sistema.



Ilustración 7.10-28

Una vez que el incidente es registrado por el sistema, al usuario se le muestra la siguiente pantalla.

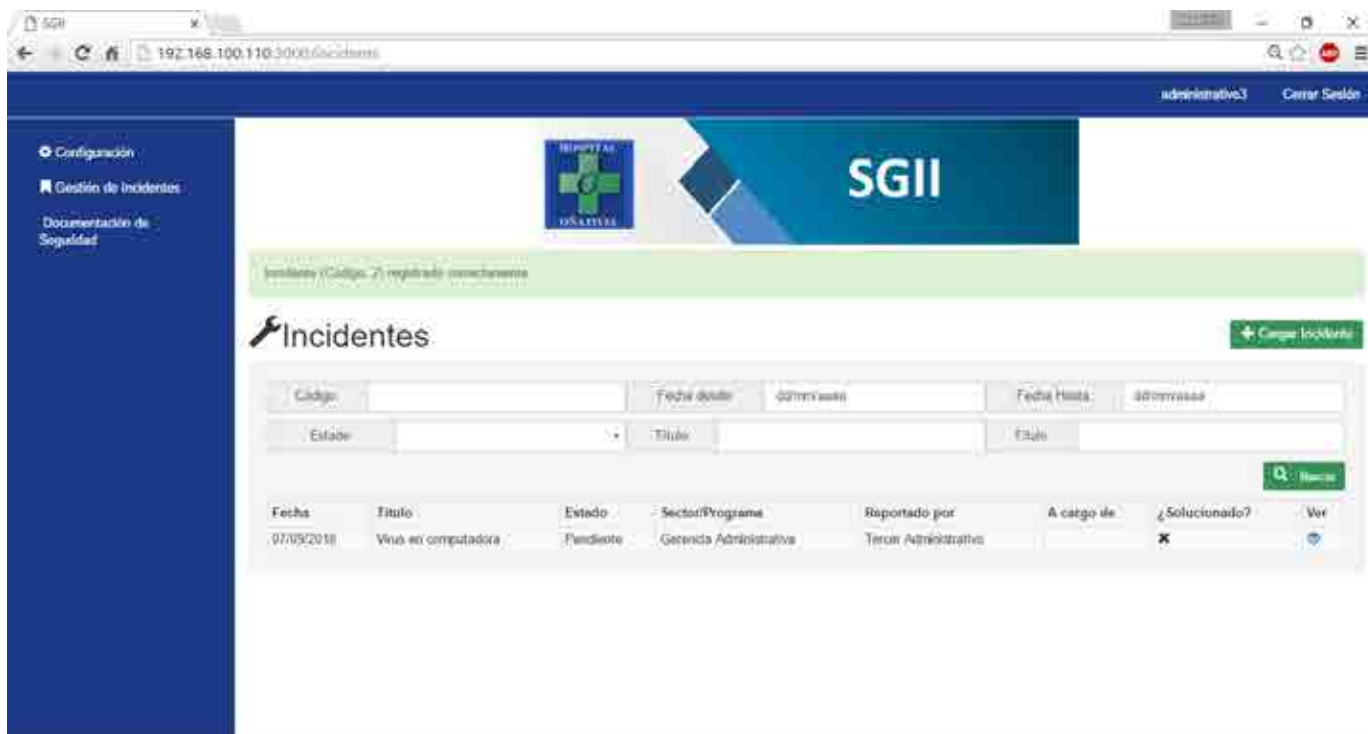


Ilustración 7.10-29

Como podemos observar en la imagen, el usuario es capaz de visualizar cierta información sobre el incidente. Además de los datos previamente ingresados (Fecha, Título, Sector/programa, Reportado por), le es suministrada información extra del incidente como ser:

- Estado: indica el estado del incidente (“Pendiente”, “En proceso”, “Solucionado”, “Desestimado”)
- A cargo de: indica la persona responsable de solucionar el inconveniente.
- ¿Solucionado?: con una cruz (X) indica que el incidente no fue resuelto, con una tilde indica que el incidente fue resuelto satisfactoriamente.

Si el usuario hubiese registrado más de un incidente, podría visualizar estos incidentes con su respectiva información, tal como se muestra en la siguiente imagen



Ilustración 7.10-30

Es posible también para el usuario, acceder a documentación relevante para la seguridad de la información. Para eso el usuario debe hacer clic en Documentación de Seguridad (Menú lateral izquierdo). Se le mostrará la siguiente pantalla.



Ilustración 7.10-31

El usuario visualizará los diferentes documentos disponibles para descargar. Si desea acceder a ellos solo deberá hacer clic en “descargar” para así obtener el archivo correspondiente.

Acciones del Administrador (Responsable de seguridad.)

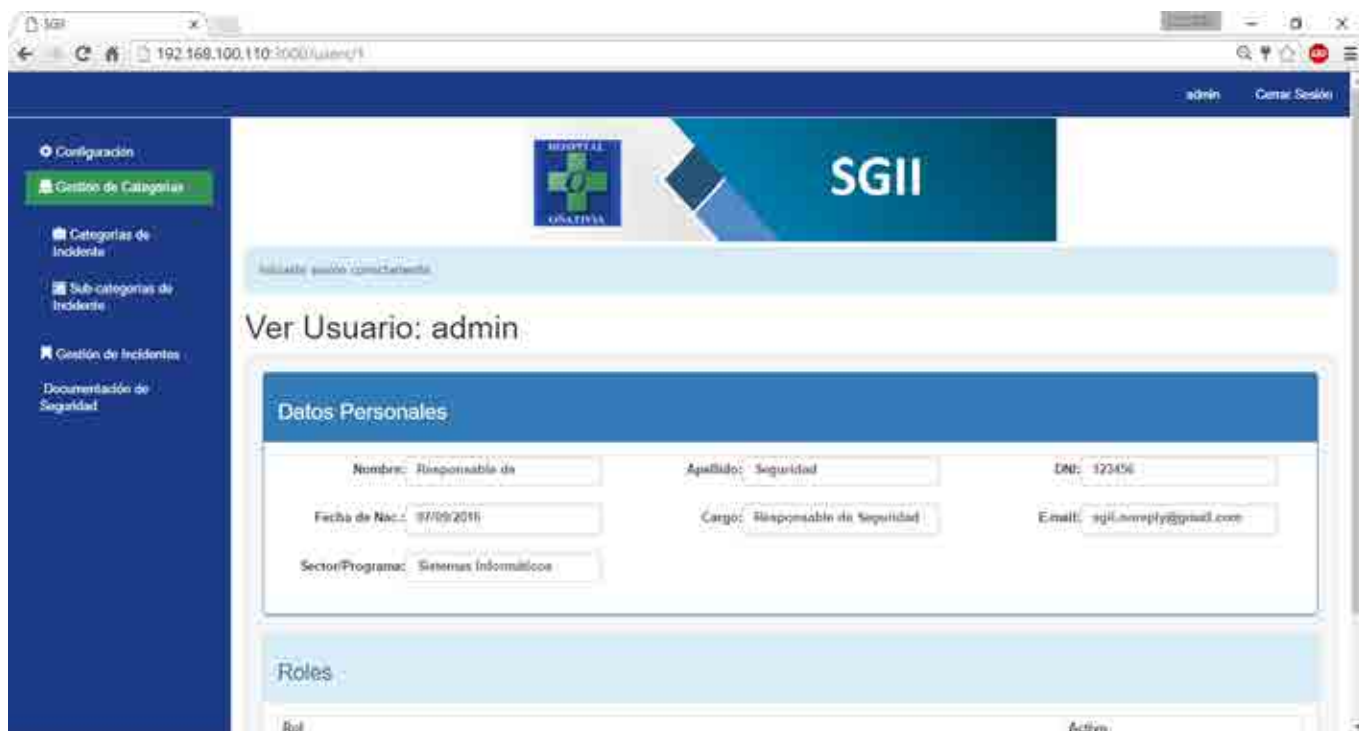


Ilustración 7.10-32

La imagen anterior corresponde a la pantalla de inicio del usuario administrador. Como podemos ver, en la parte lateral izquierda, se ofrece al administrador un menú con las diferentes características disponibles para el mismo.

En primer lugar, el administrador es capaz de gestionar las categorías y sub-categorías definidas para los incidentes de seguridad. Cuando el administrador hace clic en “Categoría de incidente” (Menú lateral izquierdo). La siguiente pantalla aparece.

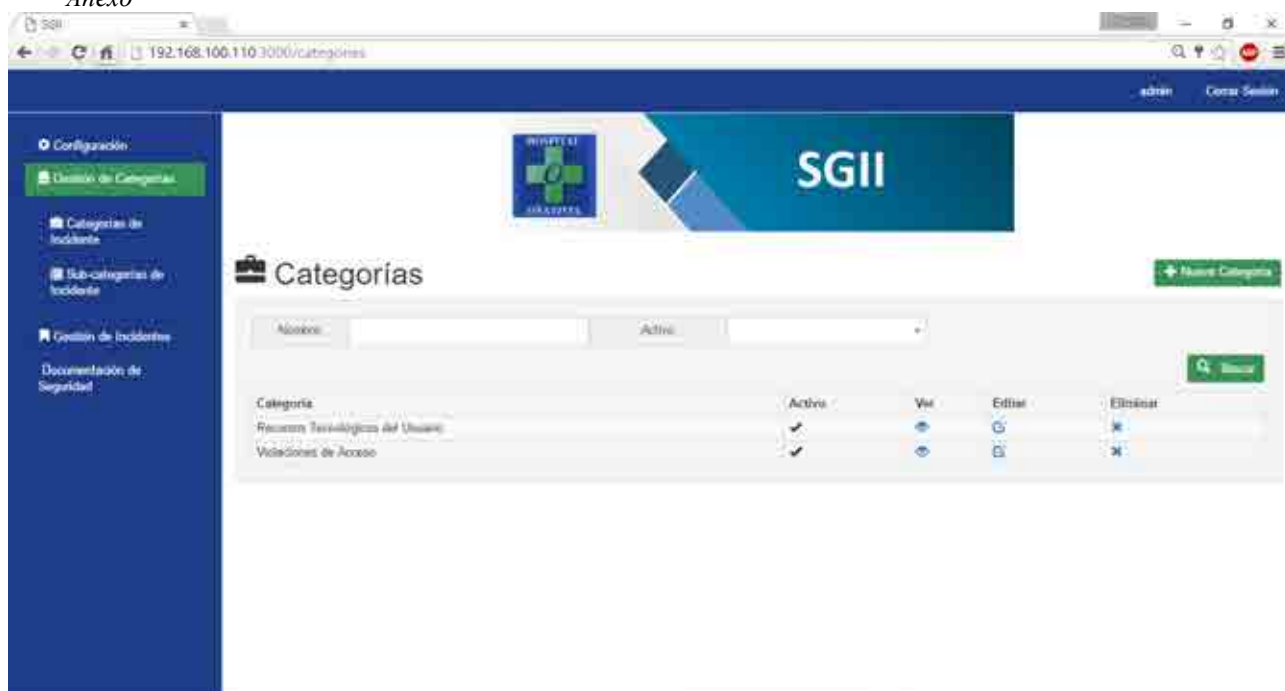


Ilustración 7.10-33

El administrador es capaz de visualizar las categorías de incidentes existentes y editar las mismas (activarlas o desactivarlas, haciendo clic en editar), eliminarlas (clic en eliminar) o bien crear una categoría nueva (clic en “Nueva Categoría”). Si desea crear una nueva categoría, la siguiente pantalla aparecerá.

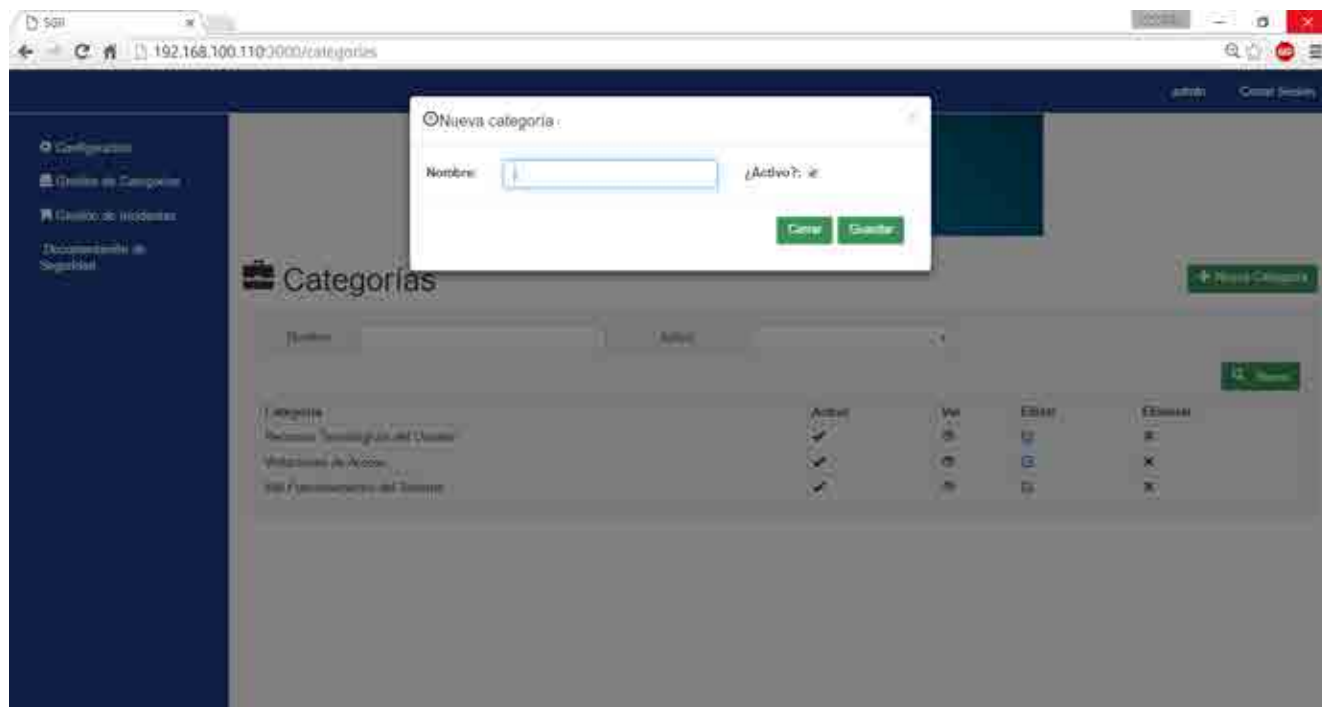


Ilustración 7.10-34

El administrador solo deberá ingresar el nombre de la categoría que desee crear, activar (o no) la misma y hacer clic en guardar para registrar la misma en el sistema.

Cuando el administrador hace clic en “Sub-Categoría de incidente” (Menú lateral izquierdo). La siguiente pantalla aparece



Ilustración 7.10-35

El administrador es capaz de visualizar las Sub-categorías de incidentes existentes y editar las mismas (haciendo clic en editar), eliminarlas (clic en eliminar) o bien crear una Sub-categoría nueva (clic en “Nueva Sub-Categoría”). Si desea crear una nueva Sub-categoría, la siguiente pantalla aparecerá.

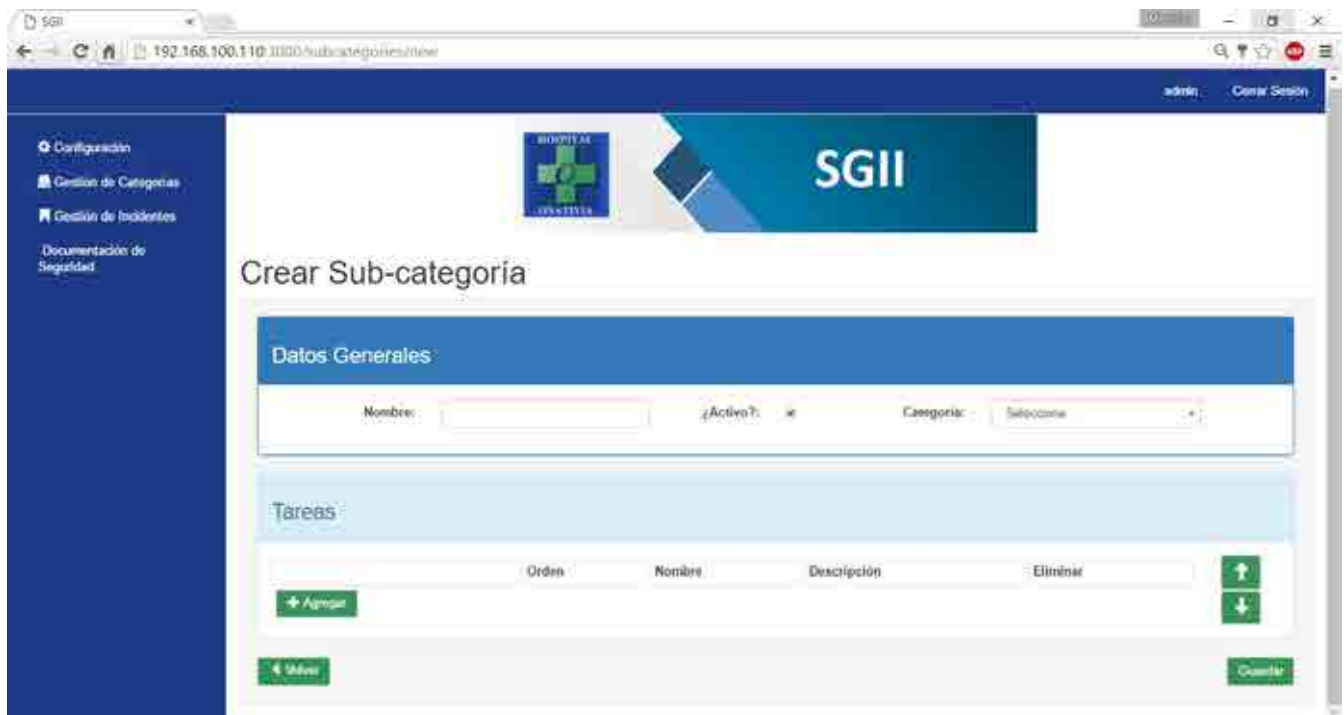


Ilustración 7.10-36

El administrador deberá, el primer lugar seleccionar la categoría a la cual pertenece la sub-categoría a crear. Una vez realizado esto, deberá ingresar el nombre de la nueva sub-categoría e indicar si esta estará activa o no en el sistema.

Deberá también ingresar las tareas a realizar para resolver un incidente identificado con dicha sub-categoría. Para esto, el administrador ingresa nuevas tareas (clic en “Agregar”) a realizar para dicha sub-categoría. El administrador definirá en base a su conocimiento y experiencia las tareas que considere necesarias para resolver un incidente de dicha sub-categoría.

Si el Administrador desea editar una sub-categoría en particular, debe hacer clic en el botón editar de la sub-categoría deseada. La siguiente pantalla aparecerá.

| Orden | Nombre                           | Descripción                                                                                   | Eliminar |
|-------|----------------------------------|-----------------------------------------------------------------------------------------------|----------|
| 1º    | Realizar Corte                   | Realizar un examen del contenido del corte eléctrico, tomando las precauciones necesarias.    | X        |
| 2º    | Añadir wires al Bloq Anti-Corona | Agregar la dirección del terminal del cable eléctrico al Bloq anti-corona de la organización. | X        |
| 3º    | Eliminar corte                   | Eliminar el cable sospechoso de la terminal del alambre.                                      | X        |
| 4º    | Verificar                        | Verifique que el cable eléctrico no sea cortado y otros cables.                               | X        |

Ilustración 7.10-37

El Administrador es capaz de editar las tareas existentes para la sub-categoría seleccionada. Es posible también eliminar las mismas o bien agregar tareas.

En el Menú lateral izquierdo, el administrador también es capaz de gestionar los incidentes de seguridad. Si hace clic en “Incidentes” la siguiente pantalla le será mostrada.



Ilustración 7.10-38

El administrador visualiza un buscador y todos los incidentes registrados en el sistema (sin importar el estado). También es posible para el administrador registrar incidentes<sup>194</sup>

El administrador es capaz de filtrar, a través del buscador, aquellos incidentes con estado “Pendiente” o el estado que desee y poder visualizar la información relacionada al incidente (clic en “ver”). El sistema permite al administrador “Categoriza y asignar” los incidentes en estado Pendiente. Para esto debe hacer clic en el botón correspondiente del incidente deseado y la siguiente pantalla le será mostrada.

<sup>194</sup> El administrador es capaz de registrar un incidente propio, o bien registrar un incidente reportado informalmente por otra persona (no se reportó el incidente a través del sistema.)

Yustman, Mauricio Ezequiel

**Categorizar y Asignar Incidente: 2**

**Datos Generales**

Código: 2 Fecha: 07/09/2018

Reportado por: administrativo3 (Tercer Administrativo) Sector/Programa: Gerencia Administrativa

Asignar a: analista1 Categoría: Recursos Tecnológicos del Usuario

Sub-categoría: Virus Informativo

Descripción del incidente:

Título descriptivo:  
Virus en computadora

Descripción del problema:  
Amplazada instalada por antivirus.  
Mal funcionamiento del equipo (Eros lema).

Ilustración 7.10-39

El administrador visualiza la información básica del incidente reportado (Código, Fecha, Reportado por, Sector/Programa, Descripción del incidente). Además de esto, este tiene la facultad de asignar un responsable (encargado de solucionar el incidente, realizar las tareas) y categorizar el incidente (seleccionar categoría y Sub-categoría). Al categorizar un incidente en particular, el sistema automáticamente vincula las tareas que son necesarias (definidas al momento de crear la sub-categoría) realizar para resolver el mismo. Una vez que el incidente fue categorizado y asignado, el estado del mismo se actualiza a “En proceso”, tal como podemos observar en la siguiente imagen.

**Incidentes**

El incidente (código 2) se asigna automáticamente

+ Cargar Incidentes

Código: Fecha inicio: 00/00/0000 Fecha fin: 00/00/0000

Estado: Título: Estado:

Sector/Programa:

Buscar

| Fecha      | Título               | Estado     | Sector/Programa         | Reportado por         | A cargo de      | ¿Solucionado? | Ver | Categorizar y Asignar | Reservar | Desactivar |
|------------|----------------------|------------|-------------------------|-----------------------|-----------------|---------------|-----|-----------------------|----------|------------|
| 07/09/2018 | Perdida de archivo   | Pendiente  | Gerencia Administrativa | Tercer Administrativo |                 | ✗             |     |                       |          | ✗          |
| 07/09/2018 | Correo Electrónico   | Pendiente  | Gerencia Administrativa | Tercer Administrativo |                 | ✗             |     |                       |          | ✗          |
| 07/09/2018 | Virus                | Pendiente  | Gerencia General        | Primer Administrativo |                 | ✗             |     |                       |          | ✗          |
| 07/09/2018 | Virus en computadora | En Proceso | Gerencia Administrativa | Tercer Administrativo | Primer Analista | ✗             |     |                       |          | ✗          |

Ilustración 7.10-40

En el Menú lateral izquierdo, el administrador también es capaz de Generar Reportes. Si el Administrador hace clic en “Reportes”, la siguiente pantalla será mostrada.



Ilustración 7.10-41

Podemos observar que es posible generar diferentes tipos de reportes:

- Incidentes por categoría: El reporte informara la cantidad de incidentes registrados en el sistema por cada categoría activa en el mismo.
- Incidentes por sub-categoría: El reporte informara la cantidad de incidentes registrados en el sistema por cada sub-categoría activa en el mismo.
- Tiempo total de resolución por sub-categoría: El reporte informara el tiempo de resolución total de cada incidente discriminado por sub-categoría.
- Tiempo promedio de resolución por sub-categoría: El reporte informara el tiempo de resolución promedio de cada incidente discriminado por sub-categoría.

En el Menú lateral izquierdo, el administrador también es capaz de cargar nueva documentación de seguridad. Si el Administrador hace clic en “Documentación de Seguridad”, la siguiente pantalla será mostrada.



Ilustración 7.10-42

El administrador, haciendo clic en “Cargar documento”, podrá seleccionar y subir el documento deseado.

Acciones del Responsable de Tareas (Analista/asignado para resolver el incidente.)



Ilustración 7.10-43

La imagen anterior corresponde a la pantalla de inicio de un usuario con responsabilidades de solución de incidentes. Como podemos ver, en la parte lateral izquierda, se ofrece al usuario un menú con las diferentes características disponibles para el mismo.

Si el usuario hace clic en “Incidentes” (Menú lateral izquierdo), la siguiente pantalla le aparecerá.

Ilustración 7.10-44

Este usuario visualiza un buscador y todos los incidentes de los cuales es responsable. Este usuario debe hacer clic en resolver (del incidente correspondiente) para visualizar la información del mismo. A continuación, se muestra dicha pantalla.

Ilustración 7.10-45

Este usuario visualiza las tareas que son necesarias realizar para resolver el incidente que le fue asignado. Además de esto, posee la facultad de marcar aquellas tareas ya realizadas, eliminar tareas que no sean necesarias realizar o bien agregar tareas que se realizaron para solucionar el inconveniente. Esto se visualiza en la siguiente imagen

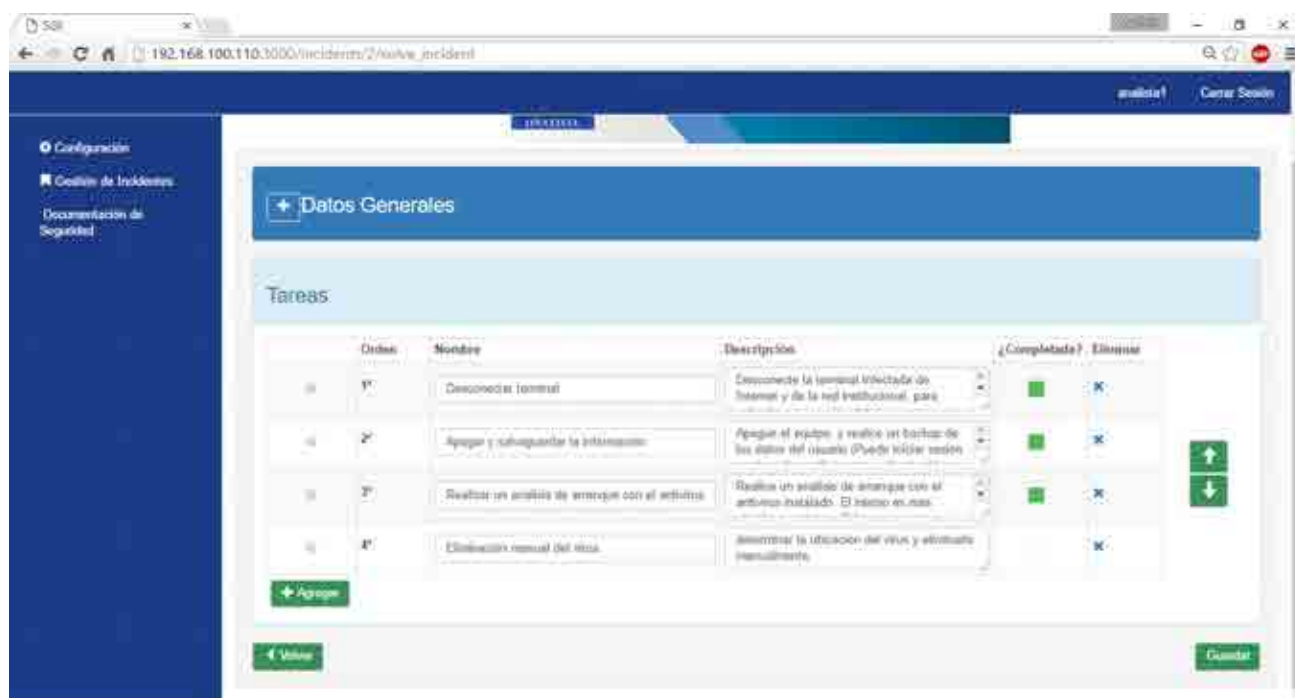


Ilustración 7.10-46

Como puede observarse, la tarea 4 fue eliminada y sustituida por una nueva (Eliminación manual del virus). Es posible apreciar también que las tareas 1, 2 y 3 están marcadas como completadas.

Una vez que todas las tareas son marcadas como completadas, una nueva opción es desplegada, tal y como se muestra en la siguiente imagen

| Orden | Nombre                                          | Descripción                                                                         | ¿Completada?                        | Eliminar                 |
|-------|-------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------|--------------------------|
| 1º    | Desconectar terminal                            | Desconecte la terminal infectada de internet y de la red institucional para         | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 2º    | Apagar y salvaguardar la información            | Apague el equipo y realice un backup de los datos del usuario (puede iniciar sesión | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 3º    | Realizar un análisis de ataque con el antivirus | Realice un análisis de ataque con el antivirus instalado. El mismo es más           | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 4º    | Eliminación manual del virus                    | Determinar la ubicación del virus y eliminarlo manualmente.                         | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

**Datos de Resolución**

Respuesta al usuario:  
El virus fue eliminado correctamente de la terminal

Fecha: 07/09/2015      Tiempo de Resolución: 2      30

Ilustración 7.10-47

Podemos observar que un campo nuevo es desplegado para completar (Datos de resolución). En dicho campo, el responsable de tarea registra un mensaje para el usuario que reporto el incidente, dicho mensaje será enviado al mail del usuario con el objetivo de notificar al mismo sobre la resolución del incidente. En el campo en cuestión, el responsable de tarea también registra la fecha y un tiempo aproximado de resolución del mismo.

Después de completado este campo, el responsable de tarea finaliza el mismo (clic en finalizar). Con esto, el estado del incidente es actualizado a “Solucionado” y se notifica al usuario correspondiente sobre la solución del mismo.



Ilustración 7.10-48

Es importante destacar que esta información será visualizada también por el administrador (Responsable de seguridad).

El responsable de seguridad tiene la facultad de visualizar toda la información relacionada a un incidente registrado en el sistema. Esto ayuda al mismo a conocer las tareas que fueron realizadas para la resolución de los incidentes y poder gestionar de manera adecuada las tareas correspondientes. En la siguiente imagen es posible apreciar, con el usuario administrador, la información del incidente solucionado.

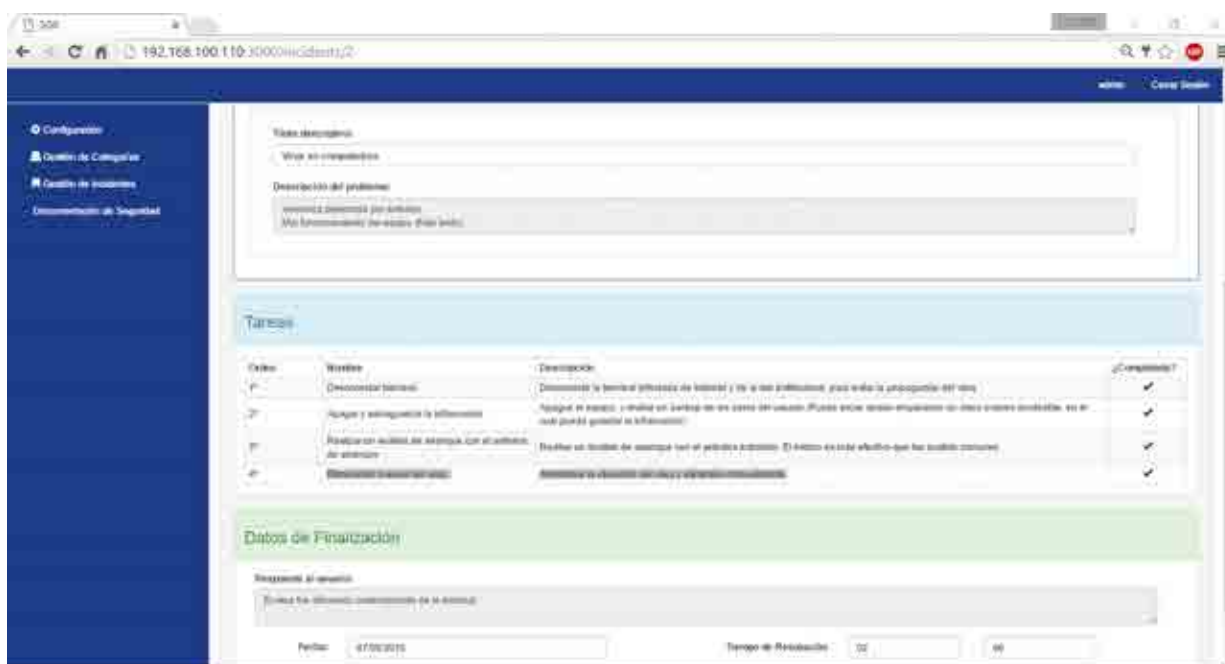


Ilustración 7.10-49