Diseño de un sistema de gestión de la seguridad informática para entorno de teletrabajo para el Instituto de Educación Superior N°2 Humahuaca- Jujuy

Ricardo C. Corimayo
ricardo_corimayo@yahoo.com.ar

Diplomatura en Seguridad de la Información Aplicada a Entornos Virtuales de Trabajo
Facultad de Ingeniería, UCASAL

Resumen

La seguridad de la información se ha convertido en un área esencial en cualquier organización, potenciado en este último tiempo por la implementación del teletrabajo. Por ello resulta importante diseñar un sistema de gestión de la seguridad de la información según las políticas marcadas por la organización, mejorando los procesos del negocio a través de metodologías adoptadas por la alta dirección que incluyen medidas organizativas, legales y técnicas; con esto se asegurará la confidencialidad, integridad y disponibilidad de la información y por, sobre todo, protegerá contra los riesgos de los activos, amenazas, vulnerabilidades e impactos. La seguridad informática en entornos virtuales se ha convertido en un factor importante en el diseño y puesta en funcionamiento del teletrabajo, donde los responsables deben implementar medidas eficaces para la seguridad de los procesos. En este trabajo se propone un plan de seguridad para el Instituto de Educación Superior N° 2 de nivel superior no universitario, donde se definirán la estructura organizacional (roles y funciones), y las políticas de seguridad para finalmente concluir con un plan de implementación, considerando aspectos tales como la virtualización, el trabajo colaborativo, servicios alojados en la nube, adecuados no solo a las políticas, sino a la implantación del teletrabajo.

Palabras Clave

Amenazas, Seguridad, Riesgos, Vulnerabilidades, Teletrabajo.

Abstract

Information security has become an essential area in any organization, enhanced in recent times by the implementation of teleworking. For this reason, it is important to design an information security management system with the policies set by the organization, improving business processes through methodologies adopted by senior management that include organizational, legal and technical measures; this will ensure the confidentiality, integrity and availability of the information, and mostly it will protect against the risks of the assets, threats, vulnerabilities and impacts. Computer security in virtual environments has become an important issue in the design and implementation of telework, where the manager of organizations must implement effective measures to keep processes safe. For this reason, in this project a security plan is proposed for the Higher Education Institute N ° 2 of a non-university higher level, where the organizational structure (roles and functions) and the security policies will be defined to finally conclude with a implementation plan, considering aspects such as virtualization, collaborative work, virtualization, services hosted in the cloud; all these are suitable not only for policies but also for the implementation of teleworking.

Keywords:

Threats, Security, Risks, Vulnerabilities, Telecommuting./

Introducción

Dentro de la estructura de cualquier organización, sea pequeña, mediana o grande se ha vuelto importante el hecho de incluir el manejo e implementación de nuevas tecnologías para automatizar sus procesos, manejo de personal, administración, capacitaciones, entre otras.

Cuando ocurre un problema dentro de la función informática en una organización, muchas de las actividades que están relacionadas con el sistema resultan afectadas, he ahí la importancia de tener una buena cultura informática y saber prevenir cualquier contingencia que se presente, para así no tener complicaciones de perder información importante.

En otros tiempos la seguridad de la información era fácilmente administrable, sólo bastaba con resguardar los documentos más importantes bajo llave y mantener instancias de seguridad de ingresos mediante guardias de seguridad. Hoy en día es más difícil.

Los sistemas electrónicos entraron en nuestra sociedad y obligaron a los sistemas de seguridad a evolucionar para mantenerse al día con la tecnología cambiante. Este trabajo se aplica al caso de una institución educativa. Hace unos años, estas, aún las más pequeñas, se conectaron a Internet (una amplia red pública con pocas reglas y sin guardianes), no quedando ajenas a los riesgos de seguridad informática.

La seguridad es sólo uno de los componentes de la administración de riesgos - minimizar la exposición de la organización y dar soporte a su capacidad de lograr su misión. Para ser efectiva, la seguridad debe estar integrada a los procesos del negocio y no delegada a algunas aplicaciones técnicas.

Los incidentes de seguridad más devastadores tienden más a ser internos que externos. Muchos de estos incidentes involucran a alguien llevando a cabo una actividad autorizada de un modo no autorizado. Aunque la tecnología tiene cierta injerencia en limitar esta clase de eventos internos, las verificaciones y balances como parte de los procesos de la organización, son mucho más efectivos.

El presente trabajo tiene como objetivo proponer un Plan de Seguridad para una institución educativa de nivel superior no universitario, que contemple diferentes aspectos tales como la virtualización, trabajo colaborativo, virtualización, servicios alojados en la nube y su adecuación a las políticas institucionales.

2. Situación del Instituto IES N°2

El Instituto de Educación Superior N° 2 (IES N°2) se ubica en la provincia de Jujuy y tiene sedes en las ciudades de Tilcara y Humahuaca. Es una institución de carácter púbico, que ofrece carreras técnicas y de profesorados, cuyo objetivo principal es la formación integral de sus estudiantes, propulsando el desarrollo sostenible de la comunidad en la cual se encuentra inserto.

En su estructura orgánica, dentro de la Secretaria Administrativa se encuentra un Área de Sistemas, que debe encargarse de mantener la funcionalidad permanente de los diferentes sistemas de información y servicios informáticos que actualmente tiene la institución, cumpliendo las normativas vigentes. Cuenta con una infraestructura tecnológica básica, una página web donde a través de sistemas "SISDES" se asisten a los procesos administrativos y pedagógicos y una plataforma virtual basada en Moodle para las aulas virtuales. Aunque se iniciaron los procesos para incrementar la capacidad técnica de la infraestructura informática, respondiendo a un plan a mediano plazo, como resultado del contexto de pandemia actual, se tuvieron que reconfigurar las expectativas de trabajo con estos sistemas, ya que no solo debía atenderse el funcionamiento de tareas administrativas y pedagógicas, sino que surgió la necesidad del correcto tratamiento de la información que resultan de las actividades de trabajo remoto de sus empleados. Sin embargo, estas transformaciones no siempre se abordan desde una perspectiva profesional sistémica y realista. Se presentó una gran demanda hacia la institución; una cuestión urgente que tuvo que atender fue la heterogeneidad en la condición de partida de sus docentes en cuanto

a su experiencia en el uso de las herramientas virtuales o modalidades a distancia, capacidades que además están influenciadas por las condiciones familiares, que afectan el trabajo docente.

En un breve periodo de tiempo se debió atender tanto a estos problemas como generar un entorno de trabajo integrado mediante una plataforma y que los procesos administrativos, propios de la institución, mantengan el resguardo necesario en cuanto al tratamiento de la información.

En repuesta a la situación planteada, el instituto requiere que su sistema informático brinde un espacio de intercambio docente, se constituya en un repositorio virtual que apoye a las clases online, brinde un sistema seguro de gestión para los actos administrativos involucrados en el servicio educativo, como mesas de examen, actas volantes, libro matriz, datos estadísticos etc., y por último generar las condiciones adecuadas para que sus empleados realicen sus trabajos de forma remota, asegurando la información. En la actualidad, la seguridad de la información es un objetivo de primordial importancia para ésta y todas las organizaciones, ya que se refiere a garantizar la calidad, disponibilidad, integridad y confidencialidad de su activo más preciado: la información.

La información es un activo que, como otros activos comerciales importantes, es esencial para el correcto desempeño de una organización y en consecuencia necesita ser protegido adecuadamente. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades [1].

A partir de los desafíos actuales impuestos por la situación sanitaria, resulta importante ofrecer un proceso de mejora y estabilidad a estos servicios, de los que dependen las aplicaciones disponibles para satisfacer las actividades de la rectoría y el actuar tecnológico que en general apoya todas las actividades administrativas-pedagógicas del cuerpo docente. Por ello, desde el Área de Sistemas, se deben realizar ingentes esfuerzos para mantener una mejora continua y proveer sistemas siempre disponibles y con las mejores condiciones técnicas posibles para el actuar institucional [2].

3. Plan de Seguridad Propuesto

En este apartado se incluyen todos los aspectos técnicos involucrados en la definición de un Plan de Seguridad Informática, para una institución como la indicada.

3.1. Objetivo del Plan de Seguridad propuesto

Este trabajo se encamina a definir las bases para un plan integral que marque los lineamientos progresivamente aplicables, a fin de lograr un Plan de Seguridad Informática, partiendo desde las copias de seguridad, sus protecciones, integralidad, restricción de acceso y demás elementos para tener en cuenta.

Se enfoca principalmente en el aspecto de la Seguridad de la Información de los componentes relevantes del sistema de Información del IES N° 2, aplicable tanto al área administrativa como la académica y sirve como marco para el trabajo pedagógico de cada docente en el diseño de sus clases virtuales, al utilizar las plataformas virtuales del instituto. Las políticas expresadas serán de obligatorio cumplimiento para todo el personal del Instituto, incluyendo sus sedes, emplazadas en localidades cercanas; será liderada por el grupo de sistemas y proporcionan las bases para la implementación y ejecución efectiva de controles que velen por la seguridad de la información, reduciendo el nivel de riesgo a la cual está expuesta, clarificando las responsabilidades de los usuarios y las medidas que deben adoptarse para proteger la información.

3.2. Caracterización del Sistema Informático de la Institución

Actualmente se cuenta con grupo de personas, encargadas del desarrollo y mantenimiento de los sistemas y un piso tecnológico que consiste en acceso a internet con un servidor proporcionado por Programas Nacionales y se contrató un servidor virtual para alojar la web y plataforma Moodle de la institución.

La red implementada está compuesta por

40 Access Point con acceso a internet, que se encuentran ubicados en aulas, oficinas y salones comunes tanto en la sede central como el resto de las sedes.

Con respecto al área de seguridad informática recientemente constituida, los roles y responsabilidades no han sido formalizados y las tareas desempeñadas se limitan por ahora al control de acceso de la mayoría de los sistemas del Instituto. Las tareas correspondientes a la administración de seguridad son desarrolladas por el grupo de sistemas como la administración de red, firewalls y base de datos; otras tareas son realizadas directamente por las áreas de los usuarios, y finalmente otras responsabi-lidades, como la elaboración de las políticas y normas de seguridad, concientización de los usuarios, monitoreo de incidentes de seguridad, etc., no han sido asignadas formalmente a ninguna de las áreas.

En este sentido, en el presente trabajo se detallarán los roles y responsabilidades relacionadas a la administración de seguridad de la información que involucra, no solamente a miembros de las áreas de seguridad informática y sistemas, como administradores de seguridad de información y custodios de información, sino también a los directivos y coordinadores de las diferentes unidades como propietarios de información, y a los usuarios en general.

3.3. Diseño del plan de seguridad de la información

Para el diseño del Plan de seguridad de la información se desarrollarán un conjunto de acciones que se inician con la evaluación de riesgos y culminan con la administración de los incidentes de seguridad. A continuación, se detalla cada componente:

3.3.1. Evaluación de riesgos, amenazas y vulnerabilidades

Para la definición del alcance de las políticas - estándares y con el propósito de identificar las implicancias de seguridad del uso y estrategia de tecnología, amenazas y vulnerabilidades y nuevas iniciativas del instituto, se desarrolló un conjunto de entrevistas con la rectoría del Instituto, personal del área de sistemas y el área de seguridad informática.

Producto del análisis de la información obtenida en dichas entrevistas, surgen los siguientes indicadores:

Los bienes informáticos más importantes para proteger son:

- La red de trabajo interno de la Oficina
- El servidor de aplicaciones.
- Las bases de datos del sistema administrativo - académico SISDES (de importancia crítica)
- El servicio de correo electrónico

Las amenazas más importantes para considerar de acuerdo con el impacto que pudieran tener sobre la institución son:

- El acceso no autorizado a la red, tanto producto de un ataque externo como interno.
- Pérdida de disponibilidad.
- La sustracción, alteración o pérdida de datos.
- La introducción de programas malignos.
- El empleo inadecuado de las tecnologías y sus servicios.

Las áreas sometidas a un mayor peso riesgo y las amenazas que lo motivan son:

- El local de los servidores de la red (acceso no autorizado y pérdida de disponibilidad).
- El local de oficinas administrativas y de dirección (alteración o pérdida de datos, pérdida de disponibilidad, la introducción de programas malignos, fuga de información clasificada)

3.3.2. Políticas de seguridad de información.

Con el objetivo de contar con una guía para la protección de información del instituto, se elaboraron las siguientes políticas y estándares de seguridad de la información, tomando en cuenta el estándar de seguridad de información ISO 27001 y las normas establecidas internamente por el instituto.

- Las propuestas de iniciativas encaminadas a mejorar el sistema de seguridad informática se aprobarán por Rectoría.
- El acceso a las tecnologías de la entidad será expresamente aprobado en cada caso y el personal tiene que estar previamente

preparado en los aspectos relativos a la seguridad informática.
- Los usuarios de las tecnologías informáticas y de comunicaciones responden por su protección y están en la obligación de informar cualquier incidente o violación que se produzca a su jefe inmediato superior.
- Todos los bienes informáticos serán identificados y controlados físicamente hasta nivel de componentes.

Identificación, Autenticación y Control de Acceso

Toda la información debe ser clasificada como Restringida, Confidencial, Uso Interno o General.

La clasificación de información debe ser documentada por el Propietario, aprobada por el Director responsable y distribuida a los Custodios durante el proceso de desarrollo de sistemas o antes de la distribución de los documentos o datos.

La clasificación asignada a un tipo de información solo puede ser cambiada por el propietario de la información, luego de justificar formalmente el cambio en dicha clasificación.

La información que existe en más de un medio (por ejemplo, documento fuente, registro electrónico, reporte o red) debe tener la misma clasificación, sin importar el formato.

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, verbigracia, cuando la información se ha hecho pública.

Seguridad ante software maliciosos.

El área de seguridad informática debe realizar esfuerzos para determinar el origen de la infección por virus informáticos, para evitar la reinfección de los equipos del instituto.

La posesión de virus o cualquier programa malicioso está prohibida a todos los usuarios. Se tomarán medidas disciplinarias en caso se encuentren dichos programas en computadoras personales de usuarios. Todos los archivos adjuntos recibidos a través del correo electrónico desde Internet deben ser revisados por un antivirus antes de ejecutarlos. Asimismo, está prohibido el uso de pendrivers provenientes de otra fuente que no sea la del mismo del instituto, a excepción de los provenientes de las interfaces con organismos reguladores, proveedores y el estado, los cuales necesariamente deben pasar por un proceso de verificación y control en el área de Sistemas (Help Desk), antes de ser leídos.

El programa antivirus debe encontrarse habilitado en todas las computadoras del instituto y debe ser actualizado periódicamente. En caso de detectar fallas en el funcionamiento de dichos programas éstas deben ser comunicadas al área de soporte técnico.

Es obligación del personal del IES emplear sólo los programas cuyas licencias han sido obtenidas por el instituto y forman parte de su plataforma estándar. Asimismo, se debe evitar compartir directorios o archivos con otros usuarios; en caso de ser absolutamente necesario, coordinar con los directores y/o coordinadores respectivos y habilitar el acceso sólo a nivel de lectura, informando al Departamento de Soporte Técnico.

Todo el personal debe utilizar los protectores de pantalla y/o papel tapiz autorizados por la Institución; el estándar es:

Papel Tapiz: IES N° 2 TILCARA JUJUY Protector de Pantalla: IES N° 2.

3.3.3. Diseño de arquitectura de seguridad de red.

Con el objetivo de controlar las conexiones de la red del IES N° 2 con entidades externas y monitorear la actividad realizada a través de dichas conexiones, se elabora una propuesta de arquitectura de red la cual incluye dispositivos de monitoreo de intrusos y herramientas de inspección de contenido.

Medidas y procedimientos

Son diversos los elementos considerados para implementar la seguridad de la información y la elección de los mismos depende de las características específicas del IES N° 2. Estas medidas y procedimientos persiguen identificar los bienes de acuerdo con su importancia, controlar y supervisar que sean utilizados en

funciones propias de trabajo y garantizar su protección.

Capacitación de usuarios

Es responsabilidad del área de seguridad informática promover constantemente la importancia de la seguridad a todos los usuarios de los sistemas de información. El programa de concientización en seguridad debe de contener continuas capacitaciones y charlas, adicionalmente se pueden emplear diversos métodos como afiches, llaveros, mensajes de log-in, etc., los cuales recuerden permanentemente al usuario el papel importante que cumplen en el mantenimiento de la seguridad de la información.

3.3.4. Resguardo y recuperación de la información

- Se define lo siguiente para este apartado:
- Se realizarán copias de seguridad de la información y del software que se determine y se comprobarán con regularidad.
- Garantizar un Servidor NextCloud[1] con carpetas particulares para cada usuario, en la cual se realizan backup de la información más importante de cada trabajador del IES N° 2.
- Cada trabajador será responsable de la información que guarde en el Servidor NextCloud y de la periodicidad con que realice las salvas personales.
- Los jefes de áreas son los responsables de organizar la salva de la información del área respectiva, definiendo la información a salvar y el trabajador encargado de esto.
- Cada área dispondrá de un disco externo para la salvaguarda de la información clasificada y/o limitada.

3.3.5. Administración de Incidentes de Seguridad.

Luego de reportado el incidente de seguridad, éste debe ser investigado por el área de seguridad informática. Se debe identificar la severidad del incidente para la toma de medidas correctivas.

El personal encargado de la administración de la seguridad debe realizar la investigación de los incidentes de forma rápida y confidencial. Se debe mantener una documentación de todos los incidentes de seguridad ocurridos en el instituto.

Se debe mantener intacta la evidencia que prueba la ocurrencia de una violación de seguridad producida tanto por entes internos o externos, para su posterior utilización en procesos legales, en caso de ser necesario.

4. El teletrabajo

El teletrabajo es una modalidad que unida al buen uso de las tecnologías de información y comunicación resulta muy efectiva para las organizaciones en el marco de la efectividad, calidad de vida, y productividad laboral.

"Se define el teletrabajo como el resultado de las aplicaciones de las tecnologías de información y comunicación, en donde no es importante el lugar geográfico ni la separación del empleador, por lo menos un 20% de las horas trabajadas" [3].

4.1. Implementación del teletrabajo en el IES N° 2

La implementación del teletrabajo requiere que la institución se organice y atienda a los siguientes requerimientos: Equipo de cómputo, conexión a internet (en caso de no ser trabajador offline), conexión a las bases de datos, seguridad informática (que resguardará la información de la comunidad educativa y dará confianza al colaborador de manejar esta información)

El mejor modelo que se ajusta a esta institución es el teletrabajo flexible, donde las personas puedan repartir su jornada laboral entre el instituto y su casa, de manera que exista cohesión del producto de su trabajo, que permita la integración con el equipo de trabajo, lo que genera importantes lazos que impactan positivamente en la realización de una tarea además de lograr consolidar el sentimiento de pertenencia. Otro tipo de teletrabajo que se propone, es el off line o desconectado,

1 https://nextcloud.com/

por el cual el personal del instituto trabaja desconectado del servidor central para luego hacer llegar los datos [4]. Aunque en pocas y especiales situaciones, accedan a la red mediante control de usuario y adecuándose a las recomendaciones de seguridad enunciadas.
En concordancia con lo expresado respecto a la norma de seguridad informática, se implementarán los siguientes ítems, desde el punto de vista de los dispositivos del Teletrabajador:

- Se implementará configuración sobre el firewall personal que responda a las políticas de control de la institución.
- Se mantendrá actualizado los Sistemas Operativos junto a las demás aplicaciones, haciendo hincapié en las actualizaciones de seguridad, como de los antivirus.
- En las computadoras portátiles se utilizará una segunda cuenta de usuario con privilegios limitados; se mantendrá la cuenta administrativa para tareas que así lo requieran.
- Se configurará el Bloqueo de Sesión para prevenir accesos no autorizados durante las ausencias temporales del Teletrabajador.
- Se limitará convenientemente la instalación de aplicaciones extra en el teléfono celular. También tendrán instalados software antivirus y antimalware.
- Se adoptará una política de renovación de contraseña segura, la cual podrá ser cambiada siguiendo los estándares de seguridad indicados en "Creación de Contraseñas Seguras".

4.2. Adecuaciones necesarias en la infraestructura para una virtualización segura.

Hoy más que nunca, la virtualización es una forma de simplificar el entorno de trabajo. La infraestructura informática no tiene por qué ser complicada: cada servidor, sistema operativo y aplicación satisface una necesidad en la organización. Sin embargo, gestionar todas esas licencias, el mantenimiento, los parches, las actualizaciones, la seguridad y los backups deja poco tiempo para mejorar las operaciones, añadir nuevas funciones y aportar un auténtico valor añadido a las tareas realizadas. Es factible el ahorro de tiempo gracias a la facilidad de administración o de clonación de los discos duros virtuales, que se realizarán como cualquier otro archivo, con las ventajas que esto tiene asociado [5].
El software de virtualización libera las aplicaciones de las ataduras y límites impuestos por el hardware con el que se ejecutan y permite compartir los recursos, lo que reduce enormemente la complejidad de TI.
Sin embargo, para el IES N° 2, debido a las carencias de recursos económicos y humanos, se propone la utilización de VMware[2]. Para empezar, ofrece licencias adaptadas al tamaño de la organización; además, la nueva tecnología de almacenamiento vSphere permite virtualizar el almacenamiento en sus propios servidores y la curva de aprendizaje es de solo unas horas. Tiene las siguientes ventajas:

- Simplicidad: VMware le ayuda a crear una infraestructura consolidada con menos servidores. Además, pone a su alcance herramientas automatizadas para optimizar y gestionar los entornos físicos y virtuales desde una única consola accesible desde un navegador web.
- Almacenamiento: Teniendo en cuenta que el Instituto no dispone de hardware de almacenamiento compartido.
- Mantenimiento sin interrupciones: llevando a cabo tareas de clonación, aplicación de parches, actualización, protección y reimplementación de máquinas virtuales sin interrupción del servicio

4.3. Servicio que se va a migrar en la nube

El concepto de "la informática en la nube" (conocido en inglés como "Cloud Computing") empezó en proveedores de servicio de Internet a gran escala, como Google, Amazon AWS, Microsoft y otros que construyeron su propia infraestructura. De entre todos ellos emergió una arquitectura: un sistema

2 https://www.vmware.com/ar.html

de recursos distribuidos horizontalmente, introducidos como servicios virtuales de tecnología informática escalados masivamente y manejados como recursos configurados y funcionando de manera continua [6].

Para la implementación de Cloud Computing en el IES N° 2 se propone utilizar una especie de "sistema hibrido", almacenando los datos más sensibles de forma local (que por lo general son pocos) y utilizando la nube para todo lo demás; por ello es necesario analizar para cada caso particular las necesidades propias de cada sede y departamento, para así saber si se puede utilizar con confianza la informática en la nube, estableciendo qué TICs locales se aplicarán y cuáles TICs en la nube servirán para el objetivo perseguido, logrando de esta manera una relación costo-beneficio-confidencialidad que se adapte a las exigencias requeridas.

En forma adicional a la utilización de la informática en la nube y con el fin de minimizar aún más los costos necesarios para comenzar a operar una solución basada en este modelo, se propone el uso de Sistemas Operativos "Open Source", como Linux, ya que la mayoría de los servicios en la nube funcionan en forma independiente a la plataforma o sistema operativo que se esté utilizando.

El servicio para migrar en la nube es el de almacenamiento, más específicamente el de Backup. "Copia de Seguridad" y se refiere a copiar, duplicar o multiplicar la información considerada lo suficientemente importante como para ser conservada, para poder recuperarla ante una catástrofe informática como la eliminación de archivos por un virus, crackers o bien accidentalmente [7]. Cuando sucede eso se pueda ejecutar procesos de recuperación de la información

Para llevar adelante el Backup es necesario considerar las siguientes recomendaciones:

- Es importante realizar una limpieza exhaustiva para liberar datos innecesarios u obsoletos, o sea, elegir la información o tipo de datos a almacenar.
- Otro aspecto destacado pasa por definir una estrategia de 'backup' y determinar con qué frecuencia realizar copias de seguridad en la nube (completa, incremental, diferencial o espejo).
- Asimismo, es posible elegir una configuración de 'backups' automáticos con tiempos e intervalos definidos (recordar que es una práctica que se debe hacer de forma periódica), de manera que no sea necesario hacer cada copia siempre de manera manual.

Consejos de seguridad cloud

- Comprobar en qué lugar van a estar alojados los datos: Uno de los aspectos que se debe tener en cuenta es en qué país van a estar ubicados los servidores en los que se encontrarán los archivos. Teniendo en cuenta que dicho país debe cumplir con las garantías adecuadas para la protección de datos y cumplir con las garantías que se deben aportar para la protección de la privacidad.
- Es necesario analizar que el proveedor de servicios garantiza la recuperación de los datos: La integridad y recuperación de los datos es otro asunto de gran relevancia. La empresa de servicios en la nube con la que se trabaje, debe garantizar la posibilidad de recuperar los datos y tener un buen sistema de copias de seguridad, diarias y programadas, y que facilite la recuperación de la información en caso de que se la necesite.
- Tener en cuenta las necesidades de uso de la nube: Si aumenta el peso del conjunto de datos con el que se va a trabajar, habrá que ampliar los planes (tener en cuenta el aspecto escalabilidad) para disfrutar de un rendimiento adecuado.
- Gestionar bien los permisos y el acceso al sistema: La gestión de permisos es uno de los ejes de la seguridad cloud. Se pueden proteger los archivos del sistema de almacenamiento y controlar la trazabilidad de estos, así como también establecer los permisos de usuario que se crea conveniente.
- Por último, es importante considerar el Cifrado de Datos: Una recomendación que no puede dejarse de lado es subir los datos cifrados (encriptados) para que ante un robo estos estén resguardados.

4.4. Sistemas colaborativos y redes sociales.
Las redes sociales son parte de los hábitos cotidianos de navegación de gran cantidad de personas. Por ello están presente dentro de las herramientas utilizadas en el Instituto para realizar sus tareas tanto pedagógicas como administrativas, logrando trabajos colaborativos y manteniendo una comunicación activa. Cualquier usuario de Internet hace uso de al menos una red social y muchos de ellos participan activamente en varias de ellas. En el instituto se mantiene activo el Facebook y el WhatsApp.
Sin embargo, a partir de su uso, los usuarios del IES se ven expuestos a un conjunto de amenazas informáticas, que pueden atentar contra su información o incluso su propia integridad.
Ante la creciente tendencia de los ataques informáticos a utilizar las redes sociales como medio para su desarrollo, se vuelve de vital importancia para el usuario estar protegido y contar con un entorno seguro al momento de utilizarlas [8].
En las redes sociales los integrantes de la comunidad educativa del Instituto pueden conectarse con otros para compartir información como fotografías, videos y mensajes.
Por ello se elaboró una serie de consejos para ayudar a proteger a los usuarios cuando usan redes sociales.

- Ser precavido al hacer clic en vínculos que recibe en mensajes de sus amigos en su sitio web social. Trate los vínculos en los mensajes de estos sitios de la misma manera que los vínculos en los mensajes de correo electrónico.
- Sepa qué ha publicado acerca de usted mismo; no use material que cualquiera pueda encontrar con una búsqueda rápida, respecto a datos laborales.
- Para evitar revelar las direcciones de correo electrónico de sus amigos, no permita que los servicios de redes sociales examinen su libreta de direcciones de correo electrónico
- Dé por sentado que todo lo que pone en una red social es permanente. Aún si elimina su cuenta, cualquiera en Internet puede fácilmente imprimir fotografías o texto o guardar imágenes y videos en una computadora.
- Tenga cuidado de instalar elementos adicionales en su sitio. Muchos sitios de redes sociales le permiten descargar aplicaciones de terceros que le permiten hacer más cosas con su página personal.

5. Conclusión
Del análisis realizado a la situación en cuanto a la seguridad informática del IES N° 2, se pudo observar una gran cantidad de amenazas (con origen en programa dañinos, o por vía remota) que reciben constantemente los sistemas informáticos y en particular los de entorno virtual.
Se partió del supuesto que un sistema de complejidad pequeña como es el del Instituto de Educación Superior, no posee muchos activos en riesgo, pero el trabajo condujo a cambiar este concepto, como lo dejó evidenciado en cada uno de los puntos desarrollados.
A pesar de que cualquier organización y en especial la del IES N° 2 se beneficia de todo lo que le provee las tecnologías de información, esto plantea un reto a los profesionales de la informática, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de la seguridad, controles, integridad de la información, etc.
Un sistema seguro debe ser íntegro (con información modificable solo por las personas autorizadas), confidencial (los datos tienen que ser legibles únicamente por los usuarios autorizados), irrefutable (el usuario no debe poder negar las acciones que realizó) y tener buena disponibilidad (debe ser estable).
Por ello es necesario mantener un estado de alerta y actualización permanente: la seguridad es un proceso continuo que exige aprender sobre las propias experiencias. El Instituto no puede permitirse considerar la seguridad como un proceso o un producto aislado de los demás. La seguridad tiene que formar parte de ella.
La seguridad informática en entornos virtuales se ha convertido en un factor importante en el diseño e implementación del teletrabajo.

El encargado de la seguridad debe estar constantemente implementando medidas eficaces para mantenerlas seguras con el fin de tener sistemas confiables y estables.
Pero a pesar de esto y aun con las mejores medidas de seguridad que se adopten siempre habrá amenazas en contras de los sistemas.

Referencias Bibliográficas

[1] GALEANO VILLA, Jorge Luis - ALZATE CASTAÑEDA, Cristian Camilo, *Protocolo de Políticas de Seguridad Informática para las Universidades de Risaralda*, disponible en: http://ribuc.ucp.edu.co:8080/jspui/bitstream/handle/10785/1731/CDMIST65.pdf?sequence=1.

[2] Plan Estratégico de las Tecnologías de la Información y las Comunicaciones (PETIC). 2015-2019- Resolución 8213 de 07 de diciembre de 2015.

[3] Roche Tovar, I. (2007). *La gerencia de Recursos Humanos Ante la posibilidad de implantación de una iniciativa de trabajo.* Revista Informe de Investigaciones Educativas, 21, 93-113

[4] Ortiz Chaparro, Francisco, *El teletrabajo. Una nueva sociedad laboral en la era de la tecnología*, Madrid: McGraw-Hill/Interamericana de España, 1997.

[5] Shackleford D. *Virtualization Security: Protecting Virtualized Environments.* 2012

[6] http://tecnofilos.aprenderapensar.net/2010/02/03/trabajar-en-la-nube-modelos-actuales-en-cloud-computing) [Consultado el 25/08/2020].

[7] *Computación en nube, Beneficios, riesgos y recomendaciones para la seguridad de la Información*, ENISA, 2009 http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment [Consultado el 25/08/2020]

[8] https://doble-efe.com/definicion-redes-sociales/ [Consultado el 25/08/2020]