GAP Analysis en controles de Seguridad de la Información en Institución Educativa Superior: Detección de oportunidades de mejora

Modalidad: Participación en Proyectos de Investigación

Autor: Hilzinger, Nicolás Eduardo

DNI: 39098653

Email: nicolashilzinger@gmail.com

Tutor: García, Marcelo Adrián

Año 2023

TABLA DE CONTENIDO

GAP Analysis en controles de Seguridad de la Información en Institución Educativa Superior: Detección de oportunidades de mejora

Autor

Hilzinger, Nicolás Eduardo

-nicolashilzinger@gmail.com-

Resumen

El presente trabajo se realiza en el contexto de una institución educativa de nivel superior, ubicada en la ciudad de San Miguel de Tucumán, Argentina.

Actualmente, las vulnerabilidades y los incidentes de seguridad están en un importante crecimiento en cualquier organización, por lo que se deben adoptar medidas de seguridad para evitar cualquier amenaza y reducir los riesgos de ocurrencia de algún incidente a un nivel tolerable.

Destacar también, la importancia de la seguridad de la información como una disciplina interconectada con el resto de las áreas funcionales dentro de una organización, con el objetivo de proteger a la institución de las amenazas, tanto externas como internas, que pueden perjudicar los diferentes activos de información con los que se trabaja.

En esta organización, se trabaja a diario con grandes cantidades de datos e información sensible que debe ser manejada con el adecuado cuidado y sólo por personal autorizado.

Por medio de esta investigación, se relevarán los procesos críticos tanto de la Dirección de Alumnos de la organización educativa, como también del estado en que se encuentra el centro de datos con respecto a los niveles aceptables de seguridad informática, física y ambiental. Una vez realizado este análisis, se formulará una política de seguridad de la información que será propuesta para los sectores objeto de estudio.

Palabras claves: Activos de información - seguridad - GAP Analysis - Política de Ciberseguridad.

Introducción

Con el paso de los años y el creciente fenómeno de la globalización, la seguridad de la información se convirtió en una disciplina indispensable en todo tipo de organizaciones.
En Argentina, los ciberataques se intensificaron en un 200% con respecto al último año, con

más de 10 millones de incidentes detectados. Con la actual situación bélica entre Rusia y Ucrania, se detectó un crecimiento de ataques con programas maliciosos (o malware), siendo los de mayor presencia los "*wipers*" -tipo de programa malicioso que borra la información de los sistemas atacados-. Este tipo de ataques constituye uno de los mayores peligros en la actualidad para todo tipo de organizaciones. Esta tendencia en aumento se suma a los ataques mediante Ransomware o aquellos de ingeniería social que están cada vez más establecidos entre las amenazas diarias de diferentes tipos de organizaciones.
Con el surgimiento de nuevas y disruptivas tecnologías se cambia permanentemente la forma de realizar las distintas actividades y, por consiguiente, el respectivo control y verificación de que el resultado obtenido es el deseado por parte de la organización.
En el ámbito de la educación, donde radica la importancia de garantizar la protección de los datos personales con los que se trabaja (estudiantes y profesores principalmente), se convierte en algo de vital importancia asegurar la confidencialidad, integridad y disponibilidad de esta información. Así también, mantener los procesos y su infraestructura en un nivel de funcionamiento óptimo y con la seguridad adecuada para que los distintos activos de información estén resguardados y protegidos ante posibles incidentes.
El objeto de estudio de este trabajo es una institución educativa universitaria radicada en la ciudad de San Miguel de Tucumán. Esta organización trabaja con un flujo diario y continuo de datos que son altamente sensibles tanto para el funcionamiento interno de la institución como para las partes interesadas que interactúan con ésta. Es por esto, que se requiere de un nivel de seguridad de la información adecuado para garantizar la salvaguarda de estos datos.

Problema

Como consecuencia del incremento de la modalidad remota en el trabajo, los incidentes de seguridad crecieron de manera exponencial poniendo en riesgo a los diferentes activos de información que posee una organización. Teniendo en cuenta el alto nivel de integridad que se requiere para los datos de la institución, los centros de datos, procesos y procedimientos no se encuentran correctamente alineados con los requisitos que impone una adecuada política de seguridad de la información.
Dada la naturaleza e importancia de la institución bajo estudio, la aparición de un incidente provocaría serios daños y pérdida de información crítica necesaria para el funcionamiento diario y continuo de la organización.

De la problemática ya mencionada, se desprenden las siguientes preguntas de investigación que servirán de guía para la realización de este trabajo.

- ¿Cuáles son los procesos y procedimientos efectuados en el sector administrativo de la institución?
- ¿Cuáles son los riesgos críticos a los que se enfrenta la organización en cuanto a la seguridad de la información y cómo impactan en las actividades diarias de la institución?
- ¿Qué medidas de seguridad se pueden implementar para prevenir y mitigar los riesgos a los que la institución está expuesta?

Objetivo General

Analizar el estado de los procesos críticos efectuados en la Dirección de Alumnos y en Centro

de Cómputos de la institución, así también la infraestructura utilizada para dar soporte tecnológico a los mismos.
Posteriormente, se llevarán a cabo una serie de recomendaciones de seguridad para los activos de información.

Objetivos Específicos

1. Identificar los procesos y procedimientos críticos que se llevan a cabo en el sector administrativo de la institución (Dirección Alumnos y Centro de Cómputos).
2. Analizar los riesgos a los que está expuesto el sector, y determinar en qué medida éstos afectan al normal funcionamiento de las actividades diarias.
3. Proponer una Política de Seguridad de la Información aplicable a los sectores bajo estudio.

Marco Teórico

La **información** es el activo más valioso de cualquier empresa, después del capital humano. El problema es que esa información corre el riesgo de ser dañada, o su flujo puede ser obstruido, lo que puede dar lugar a un mal funcionamiento de los distintos procesos que ocurren en una organización.

La **seguridad de la información** (Escrivá Gascó, G. Romero Serrano, R. Ramada, DJ. Onrubia Pérez, R. 2013) es el conjunto de medidas y procedimientos, humanos y técnicos, que permiten proteger los tres pilares fundamentales de la información. Estos pilares son:

- Integridad: certificar que la información y sus métodos de procesos sean exactos y completos.
- Confidencialidad: asegurar que puedan acceder a la información y modificarla únicamente los usuarios autorizados.
- Disponibilidad: permitir que la información esté disponible cuando los usuarios la requieran.

Según Laudon & Laudon (2016) un **activo de información** es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

Una **vulnerabilidad** se define como cualquier debilidad de un activo que pueda repercutir de alguna forma sobre el correcto funcionamiento del sistema informático. Estas debilidades pueden estar asociadas a fallos en la implementación de las aplicaciones o en la configuración del sistema operativo, a descuidos en la utilización de los sistemas, etc. (Escrivá Gascó, G. Romero Serrano, R. Ramada, DJ. Onrubia Pérez, R. 2013).

Escrivá Gascó, G. Romero Serrano, R. Ramada, DJ. Onrubia Pérez, R. (2013) muestra las **amenazas** como circunstancias desfavorables que pueden ocurrir y que cuando suceden tiene

consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

El **riesgo** consiste en las probabilidades de que una amenaza explote la vulnerabilidad de un activo de información y, por tanto, dañe a una organización.

Análisis de riesgos, según INCIBE (2020), es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.

El proceso de **gestión de riesgos** de seguridad, según INCIBE (2020), es un proceso que consiste en la comunicación, el establecimiento del contexto, la valoración del riesgo, el tratamiento y aceptación de este riesgo, y la revisión y monitorización por parte del personal responsable del sector.

INCIBE (2020) establece que la **probabilidad** es la posibilidad de materialización del riesgo analizado.

Según Escrivá Gascó, G. Romero Serrano, R. Ramada, DJ. Onrubia Pérez, R. (2013) un **ransomware** es un malware que permite a un ciberdelincuente tomar como rehenes datos e información. En donde el programa malicioso cifra estos datos, haciéndolos ilegibles hasta que la víctima ingrese una clave para descifrar la información, esta clave es lo que “promete” entregar el atacante a cambio de un de pago de rescate, que generalmente involucra una gran suma de dinero, generalmente por medio de criptomonedas y dentro de un límite establecido de tiempo.

Según el National Institute of Standards and Technology (NIST) de los Estados Unidos, un **incidente de seguridad** de la información se define como "un evento adverso o actividad no autorizada que compromete la confidencialidad, integridad o disponibilidad de los sistemas de información y de los datos que estos almacenan, procesan o transmiten".

Como explica Laudon & Laudon (2016), la **ingeniería social** es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados.

Según la norma ISO/IEC 27001:2013, una **política de seguridad de la información** es un conjunto de intenciones y directrices generales de una organización en relación con la seguridad de la información, que sirve como marco para el establecimiento de los objetivos de seguridad y para la implementación de controles adecuados.

La norma establece que la política de seguridad de la información debe ser:

1. Apropiada para la organización: Debe reflejar la cultura, los objetivos y el contexto específico de la organización.

2. Documentada: Debe estar formalizada y comunicada a todas las partes interesadas relevantes dentro de la organización.

3. Proporcionar una base para la acción: Debe proporcionar una base para establecer los objetivos de seguridad de la información y para el desarrollo y mantenimiento del sistema de gestión de seguridad de la información.

Marco Metodológico

Esta investigación se llevará a cabo en una institución educativa de nivel superior, ubicada en la ciudad de San Miguel de Tucumán.
Dicho trabajo tendrá un enfoque cualitativo, con un diseño de investigación - acción, ya que en primer lugar se efectuará la recolección de los datos necesarios y el estudio de la organización, para luego proponer una alternativa de solución práctica para la problemática planteada.
Las técnicas utilizadas para la recolección de los datos serán la observación directa y las entrevistas a personal interviniente en el área.

Sobre la Institución educativa superior

Esta institución fue creada a mediados de la década del cuarenta como resultado de la gestión de un grupo de jóvenes que tenían el deseo y la inquietud de ampliar sus conocimientos. Hasta ese momento se dictaba una sola carrera y en busca de jerarquizar la misma, sumado al creciente interés que generaba en la sociedad, es que se eleva un proyecto para la creación de una Facultad que la contenga.

Actualmente su oferta académica se compone de tres carreras de grado, once carreras de posgrado y seis diplomaturas. Es la única casa de estudios de nivel superior pública especializada en la ciencia que transmite en la provincia de Tucumán.

Cuenta con una Visión, Misión y valores formalizados que le permiten guiar su camino en búsqueda de la excelencia educativa, los cuales se describen a continuación.

Visión: Constituirnos como una institución académica de prestigio en las Ciencias xxxxxx con proyección nacional e internacional, formando profesionales que contribuyan al desarrollo, transformación y crecimiento de la sociedad.

Misión: Promover la excelencia académica y la formación de profesionales competentes en el campo de las Ciencias xxxxxx, capaces de generar y liderar cambios, con valores éticos necesarios para contribuir a un desarrollo socioeconómico sostenible.

Principios y Valores institucionales:

- Equidad para la consecución de los objetivos.
- Respeto entre los miembros de la Comunidad de la facultad y hacia la Sociedad.

● Conducta Ética y Profesional en el desarrollo de las actividades de cada miembro de nuestra Comunidad de la facultad.

● Innovación para estar a la vanguardia del conocimiento.

● Inclusión como herramienta de contención.

● Compromiso Social para contribuir al desarrollo, transformación y crecimiento de la Sociedad.

● Excelencia académica para lograr estándares de alta calidad en docencia, investigación, extensión y gestión.

DESARROLLO

CENTRO DE CÓMPUTOS Y DATOS

Observación

El personal trabaja en jornadas de cuatro horas diarias, de lunes a viernes. El fin de semana, un guardia se encarga del cuidado del establecimiento y de la supervisión del centro de cómputos.

La oficina se encuentra en una posición poco visible y de poco tránsito. La única entrada se encuentra permanentemente cerrada para el público en general, y cuenta con un timbre para dar acceso sólo a personal autorizado.

Dentro de la oficina, se observa una habitación bajo llave donde se encuentran los servidores utilizados y equipos tecnológicos que se utilizan.

Resultados de la entrevista

Se realizó una entrevista al profesional en Ingeniería responsable del área de sistemas de esta institución, para conocer de mejor manera como es el funcionamiento de este departamento.

El centro de cómputos de la facultad está comprendido dentro del área de desarrollo y de tecnología y seguridad. Esta área depende directamente del director de la institución.

Accesos no autorizados. La entrada a la oficina se encuentra cerrada con llave y el acceso está permitido sólo a personas autorizadas. Existe un aviso en la entrada de que dicho sector no atiende consultas al público en general.

Para evitar intrusiones en los servidores de la base de datos, se cuenta con un sistema de credenciales únicas vinculadas al correo electrónico (Gmail) de cada uno de los trabajadores autorizados.

Soporte: el sistema trabaja en la actualidad con un sistema de "tickets", que es como se denominan a las solicitudes o pedidos que ingresan en el sistema por parte de los usuarios. Estas solicitudes se registran y clasifican según su prioridad de ser atendido el reclamo. El usuario, a su vez, puede llevar un seguimiento de su ticket con el objetivo de conocer el estado de su trámite.

En cuanto a los activos de información, la base de datos es el más crítico ya que es donde se encuentra información confidencial, tanto de alumnos como de profesionales. El motor de esta base de datos (Informix) actualmente se encuentra en los servidores físicos de la institución.

Los mails utilizados por los profesionales de este departamento se encuentran en un servicio de nube (Gmail).

Todo el inventario de activos de información depende de una sección llamada Bienes del estado que es manejada por la secretaría de administración y depende del estado nacional.

Escaneo de vulnerabilidades: De manera periódica, son efectuados escaneos sobre el sistema de autogestión de alumnos (SIU) en busca de vulnerabilidades.

Al estar segmentadas las redes Wifi utilizadas, la presencia de vulnerabilidades en dicho sector es más probable que ocurran de manera física.

Los equipos tecnológicos del sector de laboratorio se encuentran frisados para evitar accesos no autorizados o sospechosos en determinados sitios web.

Segmentación de redes: Se utiliza un sistema de Virtual Private Network (VPN) para las redes Wifi. La red utilizada por el centro de cómputos es diferente de aquella utilizada por estudiantes o por el resto de la organización a un nivel físico (utilizan redes con cableado diferente). Se les aplicó un proceso de endurecimiento (hardening) con el objetivo de reducir los peligros y amenazas.

Seguridad ambiental: Se cuenta con matafuegos especiales para que, en caso de ser necesario, se utilicen sin riesgo de dañar los dispositivos electrónicos. También existe un sistema de refrigeración especial en la sala de servidores.

La ausencia de una alarma de humo en el sector de los servidores constituye un gran riesgo para el funcionamiento óptimo de estos equipos, debido a que están en funcionamiento el día completo y son así susceptibles de producir cortocircuitos o incendios.

Back-up: Existen dos tipos de respaldo de información que se detallan a continuación.

- Con respecto a la base de datos, se efectúa una copia de seguridad diaria que es realizada hora por hora para mantener segura la información crítica que entra

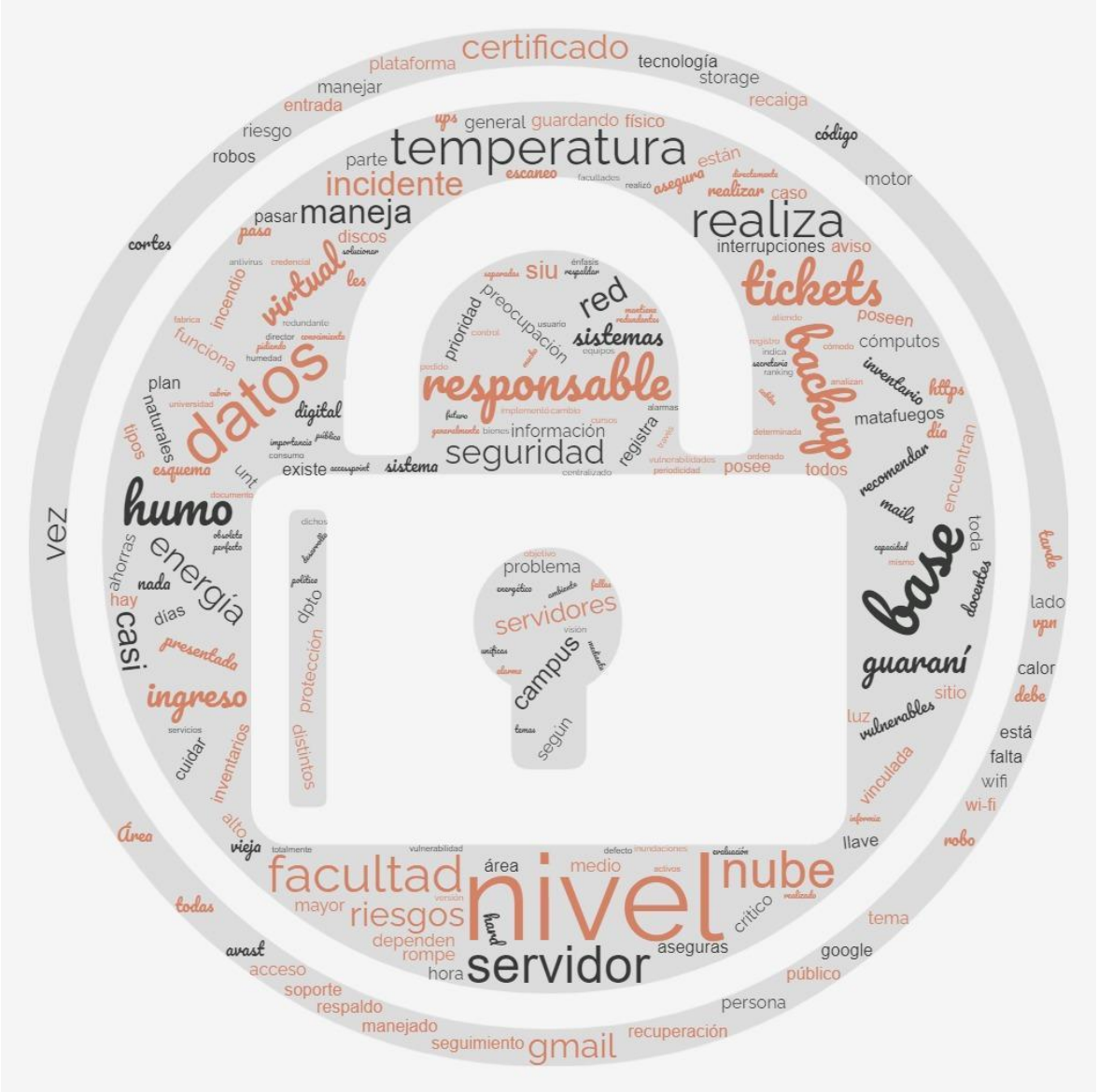
permanentemente en la institución. En cuanto al servidor completo, se realiza un backup cada siete días.

Existe un backup histórico sobre los Excel trabajados por parte del personal del departamento que sirve como respaldo ante una pérdida o necesidad de alguna información específica pasada.

- A nivel del sitio web de la organización, se realiza un respaldo de la información tanto de la base de datos utilizada en el sitio como del resto de actividades realizadas en el sitio web de la facultad.

Disponen de dos dispositivos centrales de almacenamiento físicos (storage) con redundancia de cinco discos en donde se respaldan los datos.

Título: Nube de palabras



Fuente: elaboración propia.

ANÁLISIS DE RIESGOS

De la información recopilada por medio de la entrevista y de la observación directa en el área de trabajo, se procede a elaborar un análisis y clasificación de los principales riesgos a los que está expuesta el área de cómputos de esta institución.

Este análisis se desarrollará en función a la clasificación de los principales riesgos de acuerdo a una matriz donde se mide la probabilidad de ocurrencia y la severidad o impacto de estas situaciones.

Esta herramienta es muy útil para conocer la probabilidad de ocurrencia de ciertos eventos y clasificarlos según su criticidad y severidad al momento de aparición. Conocer esta

clasificación, permite a los responsables tomar decisiones sobre aquellas situaciones que están al límite y evitar así una situación desafortunada que pueda provocar serios daños en la organización.

Título: Matriz de riesgos

		SEVERIDAD		
		Baja	Media	Alta
PROBABILIDAD	Baja	Trivial	Tolerable	Moderado
	Media	Tolerable	Moderado	Alto
	Alta	Moderado	Alto	Muy alto

Fuente: elaboración propia

De acuerdo al análisis realizado, los principales riesgos destacados y su clasificación son los siguientes:

1. Temperaturas de los servidores. Si bien el departamento de cómputos cuenta con un sistema de refrigeración adecuado, es una de las principales preocupaciones, debido a que los servidores y artefactos utilizados son muy sensibles al calor y su funcionamiento (las 24hs del día, los 7 días de la semana) se puede ver gravemente afectado de generarse una temperatura muy elevada. Por esto es que se asigna la clasificación máxima de riesgo (probabilidad alta, impacto alto).
2. Riesgo de incendios. Un cortocircuito en un equipo electrónico o un error humano producto de un descuido o negligencia, puede generar un principio de incendio que puede provocar graves consecuencias tanto a equipos como a información presente en el lugar. Clasificamos este riesgo con una probabilidad de ocurrencia media y un impacto resultante alto.
3. Ataques de Malware: uno de los más destacables es el Ransomware que se refiere al malware que permite a un estafador tomar como rehenes datos e información. En donde el programa malicioso cifra estos datos, haciéndolos ilegibles hasta que la víctima ingrese una clave para descifrar la información, esta clave es lo que "promete" entregar el atacante a cambio de un de pago de rescate, que generalmente involucra una gran suma de dinero, generalmente por medio de criptomonedas y dentro de un límite establecido de tiempo. La probabilidad de que sucedan es media pero el impacto es alto.
4. Robos de equipos. Este es siempre un riesgo a tener en cuenta debido al alto valor monetario que tienen los equipos tecnológicos que se encuentran en esta institución. Se clasifica a este riesgo con una probabilidad de ocurrencia media y un impacto medio.
5. Interrupción del suministro de energía eléctrica. Es una situación común en la provincia donde está ubicada la Facultad, especialmente en los meses de primavera-verano donde por las elevadas temperaturas la demanda de energía es mayor y se producen cortes programados o no programados. La probabilidad de que sucedan es alta pero el impacto es bajo.

Tabla: Clasificación de riesgos

Ranking	Riesgo	Probabilidad de ocurrencia (P)	Severidad o impacto (S)	Clasificación de riesgo (P x S)
1	Temperatura de servidores	Alta (3)	Alta (3)	Muy Alto (9)
2	Incendios	Media (2)	Alta (3)	Alto (6)
3	Ataques de malwares	Media (2)	Alta (3)	Alto (6)
4	Robo de equipos	Media (2)	Media (2)	Moderado (4)
5	Interrupción energía eléctrica	Alta (3)	Baja (1)	Moderado (3)

Fuente: Elaboración propia

DIRECCIÓN ALUMNOS

Para el análisis de esta sección se llevará a cabo una entrevista al personal interviniente en esta área de trabajo con el objetivo de conocer el estado de los procesos críticos de seguridad de la información que se desarrollan allí.

Para este sector, se utilizará como referencia los Controles de Seguridad Crítica de CIS. Esta herramienta es un conjunto prescriptivo y prioritario de las mejores prácticas de seguridad cibernética y acciones defensivas que ayudan a prevenir de ataques maliciosos, y ayudan al cumplimiento de múltiples marcos de referencia.

Los Controles de CIS proporcionan una orientación específica para que las organizaciones alcancen sus metas y objetivos descritos por diversos marcos jurídicos, reglamentarios y normativos.

Esta herramienta divide a las organizaciones y empresas según tres categorías de autoevaluación (IG) en cuanto a su tamaño y experiencia en IT y seguridad. Cada uno de los IG superiores contiene o incluye al anterior. Estas categorías son:

- **IG1**. Lo constituyen empresas con un nivel de seguridad de la información básico, generalmente organizaciones de tamaño pequeño a mediano. La principal preocupación de estas empresas es mantener el negocio operativo.

- **IG2**. Empresas donde se encuentran encargados de administrar y proteger la infraestructura de IT, con un apoyo interdepartamental en cuanto a los diferentes perfiles de riesgo. Se almacena la información sensible de clientes internos o externos. Su mayor preocupación es perder la confianza del público ante una brecha.
- **IG3**. Emplean expertos en seguridad especializados en distintos aspectos de ciberseguridad. Este tipo de empresa debe abordar la disponibilidad, confidencialidad e integridad de los datos sensibles.

Análisis en base a controles críticos de CIS

Se realiza un análisis de los procesos y procedimientos efectuados en la institución en base a los principales controles críticos de CIS. Estos controles incluyen las distintas herramientas que debe tener en cuenta la organización para prevenir y mitigar los diferentes riesgos que se presentan.

Posterior a este análisis, se presentan posibles alternativas de solución a los problemas encontrados en el estado de los procesos de la institución.

1. Inventarios y control de activos empresariales

La información no es clasificada según su importancia y/o confidencialidad, existe un tratamiento igualitario para toda dicha información con que se trabaja.

En cuanto al inventario de servidores y equipos, éstos pertenecen a la sección de Bienes del Estado, la cual está regida por la ley del estado nacional.

Acciones correctivas:

Se recomienda identificar y mantener un inventario actualizado de la información crítica que se maneja en sección alumnos, clasificando a la misma según su confidencialidad y/o criticidad. Esto permitirá dar un tratamiento distintivo a aquellos activos de información considerados sensibles para la organización y sus partes intervinientes.

2. Inventarios y control de activos de software

No todo el software autorizado cuenta con la licencia del fabricante. Periódicamente, se realiza un escaneo de los equipos de trabajo con el fin de detectar y evitar la presencia de software no autorizado o aplicaciones indebidas.

Existen restricciones en los equipos electrónicos al momento de intentar descargar software o aplicaciones no autorizadas o no relacionadas con las actividades realizadas por el sector.

Acciones correctivas:

- Establecer y mantener un inventario del software autorizado donde se deberá indicar, principalmente, el título del software, el editor, la fecha de instalación y la versión del programa.
- Es recomendable revisar y actualizar este inventario al menos con una periodicidad de dos veces al año.

3. Protección de datos

No existe una política de uso para el tratamiento de los activos de información. El acceso a los equipos tecnológicos del sector se lleva a cabo mediante usuario único de cada individuo autorizado.

No se clasifica a la información según su criticidad o privacidad. El tratamiento es el mismo para todo tipo de datos que sean manejados en este sector.

La información de la base de datos no es compartida con personal ajeno no autorizado a dirección alumnos, salvo excepciones de fuerza mayor, sólo con autorización explícita de la parte autorizada.

No se encuentra cifrada la información en reposo ni aquellas proveniente de medios extraíbles.

La modificación de información sensible se produce mediante previa solicitud vía acta formal. Una vez realizada la edición, queda registrada en una nueva acta rectificada.

Acciones correctivas:

- Se recomienda establecer y mantener un proceso de gestión y de inventario de datos con el fin de abordar la confidencialidad de los datos, el propietario y manejo de los mismos, y los requisitos para la eliminación de información establecidos por la organización.
- Identificar, documentar e implementar reglas para el uso aceptable y manejo de los distintos tipos de información.
- Establecer un proceso de eliminación de la información inutilizada acorde al grado de sensibilidad de los datos.
- Se recomienda clasificar la información de acuerdo a las necesidades de la seguridad de la información de la institución en función de la disponibilidad, integridad y confidencialidad de dicha información.

4. Administración de cuentas

Las cuentas utilizadas en los sectores de la institución se utilizan mediante el uso de contraseñas individuales.

Actualmente, no existe un procedimiento formal para dar de baja o eliminar aquellas cuentas de correo electrónico inactivas o que ya no se utilizan.

Acciones correctivas:

- Establecer un procedimiento formal de eliminación o inhabilitación de cuentas inactivas luego de un periodo de 45 días de inactividad.
- Centralizar la gestión de cuentas utilizadas en la organización a través de un directorio o comité responsable.

5. Gestión de control de accesos

No hay un proceso formal que exija múltiple factor de autenticación para el acceso a las aplicaciones institucionales.

No está permitido el acceso remoto a la red o a las distintas aplicaciones relacionadas con la institución.

Existe un nivel de autoridad para el acceso a actividades sensibles como ser la modificación o eliminación de cierta información.

Existen ciertas actividades a realizar en los sistemas y en el sitio web que son realizadas sólo por el encargado del sector de sistemas.

Acciones correctivas:

- Establecer un proceso para otorgar acceso a los activos de la organización en caso de nueva contratación o cambio de funciones de un usuario.
- Implementar procesos de tecnologías de autenticación segura en función de las restricciones de acceso a la información de cada usuario de la institución.

6. Gestión continua de vulnerabilidades

En la institución, no hay un proceso documentado de gestión de vulnerabilidades.

Se realiza un escaneo periódico dentro de la red y en el sistema de autogestión de alumnos en busca de riesgos o vulnerabilidades.

Se utiliza una versión obsoleta del sistema de gestión de alumnos.

Acciones correctivas:

- Establecer y mantener un proceso documentado de gestión de vulnerabilidades para los activos de la organización. Revisar dicha documentación anualmente.
- Realizar actualizaciones del sistema operativo en los activos de la institución, como por ejemplo en el sistema de autogestión de alumnos de la organización.
- Establecer procedimientos formales de exploración de vulnerabilidades automatizadas de activos internos de la facultad, con una periodicidad trimestral o de mayor frecuencia.

7. Protección de correo electrónico y Defensa contra Malware

Se instalaron software antivirus y firewalls en los equipos de trabajo del sector.

No hay un protocolo formal para deshabilitar o eliminar navegadores o complementos de correo electrónico no autorizados o que ya no se utilizan.

Acciones correctivas:

- Restringir, mediante desinstalación o desactivación, cualquier complemento o aplicación no autorizado o innecesario del navegador o del correo electrónico.
- Configurar el software anti-malware para escanear automáticamente los medios extraíbles.

8. Recuperación de datos y copias de seguridad

La política de copia de seguridad se realiza en dos dispositivos de almacenamiento externos. La base de datos del sistema de autogestión tiene un backup diario programado que se realiza cada una hora, mientras que la copia de seguridad del servidor se efectúa con una frecuencia de siete días.

A nivel del sitio web de la institución, el backup se realiza tanto sobre la base de datos como sobre el sitio completo en sí.

Existe un backup histórico sobre las plantillas de Excel con que se trabaja en el sector, con el fin de tener un auxilio en caso de necesidad o pérdida de información.

9. Gestión de infraestructura y monitoreo de redes

La arquitectura de red utilizada para el funcionamiento del sitio web principal de la institución cuenta con un protocolo seguro (https). Mientras que el sistema de autogestión para los alumnos no utiliza un protocolo de internet asegurado.

Las tareas administrativas de los sectores objeto de estudio se realizan mediante una previa autenticación a la VPN, para lograr un acceso de manera segura.

Acciones correctivas:

- Asegurar y mantener actualizada la infraestructura de red de la institución, ejecutando siempre las últimas versiones del software utilizado, entre otras implementaciones. Revisar periódicamente las versiones de las distintas aplicaciones con que se trabaja.
- Establecer y mantener recursos informáticos dedicados, separados física y lógicamente, para todas aquellas tareas y actividades que requieran de permisos de administrador. Los recursos deben estar separados de la red principal de la empresa.

10. Concientización y capacitación en seguridad

No se realizan capacitaciones en materia de seguridad de la información a los distintos colaboradores de los sectores estudiados.

No hay un proceso formal de concientización en cuanto a un reconocimiento de las diferentes técnicas de ingeniería social o errores humanos que pueden presentarse.

Actualmente, no existe una capacitación en lo referido a identificar, almacenar, archivar la información sensible y confidencial con que se trabaja.

Acciones correctivas:

- Establecer y mantener un programa de concientización sobre seguridad, con el objetivo de educar a la fuerza laboral sobre cómo interactuar con activos y datos de la organización de forma segura.
- Capacitar a los colaboradores para reconocer diferentes ataques de ingeniería social, como el phishing, mensajes de texto o seguimientos.
- Capacitar sobre las mejores prácticas en autenticación, contraseñas y credenciales seguras.
- Capacitar a los miembros de la institución para que puedan reconocer e informar un incidente potencial.

11. Gestión de respuesta a incidentes

No fue designada formalmente la persona que tendrá a su cargo la gestión de incidentes de la institución.

La organización carece de una asignación formal de roles y responsabilidades para responder en caso de incidentes.

Acciones correctivas:

- Designar una persona clave que administrará formalmente el proceso de manejo de incidentes de la facultad. Debe ser responsable de la coordinación y documentación de las respuestas a incidentes y de los esfuerzos de recuperación.
- Planificar y realizar escenarios de respuesta a incidentes de rutina para el personal clave del sector para prepararse para responder ante incidentes reales.
- Realizar revisiones posteriores a incidentes para evitar la recurrencia de los mismos mediante la identificación de lecciones aprendidas y acciones de seguimiento.

12. Gobierno y gestión estratégica

No existe una política formal de seguridad de la información.

No se ha designado a un responsable de guiar a la organización en los temas referidos a la seguridad de la información.

La institución carece de un comité de seguridad que se encargue de tratar los temas específicos que surjan en materia de seguridad.

Acciones correctivas:

- Implementar una política de seguridad de la información con el fin de proteger los recursos de la organización, asegurar la continuidad de la institución, y cumplir su misión y objetivos estratégicos en materia de seguridad.
- Formar y mantener un comité de seguridad que sea responsable de impulsar, velar y responder por la seguridad de la información de la institución educativa. Este comité debe ser liderado por un responsable formalmente designado para el puesto, que tenga a cargo toda el área de seguridad de la información de la organización.

13. Política de contraseñas seguras

Cada trabajador del sector tiene su usuario y contraseña única con la que ingresan al sistema y realizan sus actividades.

No existen contraseñas grupales o genéricas.

Acciones correctivas:

- Mantener un inventario de gestión de las contraseñas utilizadas por los colaboradores en los distintos sistemas informáticos, con el fin de tener un registro de acceso a los sistemas.
- Definir y aplicar reglas de escritorios y pantallas libres de documentos y de medios extraíbles para las instalaciones de procesamiento de información.

14. Seguridad física

El acceso físico a los sectores se encuentra restringidos para personal ajeno a dichas áreas.

Los sectores cuentan con medidas físicas en caso de accidentes.

El área de sistemas no cuenta con una alarma de humo y un sistema que alerte cuando se sobrepase cierta temperatura límite de los servidores.

Se cuenta con refrigeración adecuada tanto en sección alumnos como en área de servidores y sistemas.

Acciones correctivas:

- Implementar y asegurar la seguridad física de oficinas, salas e instalaciones.
- Realizar monitores continuamente para detectar accesos físicos no autorizados.
- Diseñar e implementar protecciones contra amenazas físicas y ambientales, como desastres naturales u otras amenazas físicas intencionales o no intencionales a la infraestructura de la organización.

PROPUESTA DE MEJORA

Una vez realizado el estudio y análisis de los sectores de la institución y sus diferentes procesos y procedimientos realizados, se ofrece una alternativa para la optimización del nivel de seguridad de la información en dicha organización. Dicha alternativa consiste en la propuesta de una política de seguridad de la información que contenga las directrices y reglas establecidas por la organización para garantizar la protección adecuada de la información y de los recursos relacionados.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. ALCANCE

La presente política, en sujeción a las normativas internacionales en este campo y en cumplimiento de las regulaciones legales vigentes nacionales, se debe aplicar a cada una de las actividades y recursos en donde se procesen y almacenen datos e información, ya sean gestionadas por un soporte manual o uno automatizado, que estén bajo el dominio de la Facultad.

La misma debe ser comunicada de manera efectiva a toda la comunidad educativa, la cual se entiende que está formada por: docentes, personal no docente y alumnos.

2. PRINCIPIOS BÁSICOS

Los principios que guían los lineamientos expresados en este documento son los siguientes:

● Confidencialidad: debe garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

● Integridad: se debe salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.

● Disponibilidad: debe garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Uno de los principales objetivos que se buscan es el de proteger los datos personales procesados, así como cualquier otro tipo de información sobre la que sea responsable la institución.

Las autoridades máximas del centro educativo se deben comprometer a llevar a la práctica lo expresado en este escrito, buscando lograr una mejora continua en la forma de gestionar la seguridad de la información, en búsqueda constante de lograr maximizar eficacia y eficiencia en su gestión.

Los requisitos de seguridad que se desarrollarán serán fijados con base en un análisis pormenorizado de las condiciones específicas de la organización.

3. REVISIÓN Y ACTUALIZACIÓN

Es necesario que la política de seguridad de la información sea revisada de manera periódica para lograr una acertada gestión de riesgos, ya que los tipos de incidentes posibles van evolucionando con el tiempo, y es necesario estar preparados para afrontar las situaciones problemáticas, siendo deseable (y preferible) actuar de manera preventiva.

Los responsables de emprender las acciones de revisión y actualización son los integrantes del Departamento de Sistemas de la institución, de manera colaborativa con el Honorable Consejo Directivo de la Facultad.

Se establece que debe ser llevada a cabo obligatoriamente de manera anual. Resulta imprescindible dejar constancia de cualquier cambio por más pequeño que sea y de que este ha sido comunicado a las partes interesadas.

4. LINEAMIENTOS ESPECÍFICOS

4.1 **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.**

4.1.a. Comisión de Seguridad de la información.

La citada comisión estará formada de manera conjunta por los miembros del Consejo Directivo y el Departamento de Sistemas. Esto con la finalidad de que se logre un equipo multidisciplinario que realice aportes diversos y enriquecedores para la protección de la información procesada en toda y cada una de las actividades desarrolladas en la institución.

4.1.b. Funciones de la Comisión de la Seguridad de la Información.

● Revisar la presente política de manera periódica, en búsqueda de la mejora continua.

● Asegurar la correcta comunicación e implementación de la presente normativa.

● Llevar a cabo el análisis de criticidad de los activos de información de los cuales es dueña la Facultad.

● Promover la concientización y capacitación en materia de Seguridad de la Información.

● Establecer los procesos y controles que sean necesarios para asegurar la protección de la información.

4.2 **SEGURIDAD DE LOS RECURSOS HUMANOS**.

4.2.a Definición de puestos.

En cada descriptivo de puestos se debe incluir:

● Activos de información asociados al cargo.

● Competencias requeridas.

● Cada tarea asociada con su correspondiente responsabilidad en materia de seguridad de la información.

4.2.b Controles y capacitación.

El jefe de cada área es el encargado de vigilar la adhesión y cumplimiento de las normas de seguridad de manera más incisiva. También es su deber detectar puntos débiles en el trabajo de sus subordinados y coordinar las jornadas de capacitación que sean necesarias para remediarlos.

4.2. c Convenio de confidencialidad.

Sin importar el cargo que se ocupe ni el nivel jerárquico del mismo, todo el personal que tenga algún tipo contacto con los activos de información de la institución deberá firmar al iniciar su relación laboral un contrato de confidencialidad, con el fin de asegurar la no divulgación y protección de la información de la que es responsable el centro educativo.

4.3 **GESTIÓN DE ACTIVOS.**

4.3.a Inventario de activos.

Es fundamental contar con un listado de los activos de información que posee la institución especificando su ubicación y quien es el responsable del mismo. Se debe revisar y actualizar cuatrimestralmente.

4.3.b Clasificación de la información.

El criterio con el que se llevará a cabo la clasificación estará basado en las tres principales características de la información: confidencialidad, integridad y disponibilidad, siguiendo el método que se detalla a continuación:

CONFIDENCIALIDAD

0- Información autorizada para ser de dominio público, por lo cual puede ser conocida y manipulada por cualquier usuario. PÚBLICA.

1-Información a la que tiene acceso solo personal autorizado y cuya divulgación o acceso no autorizado representa un error leve. RESERVADA.

2- -Información que si es divulgada afecta los intereses de la Facultad. Es de jerarquía gerencial. CONFIDENCIAL.

3-Información que por su importancia requiere un nivel de protección mayor porque su divulgación representa un grave error y provocaría un daño excepcional a la institución. SECRETA.

INTEGRIDAD

0-Información cuya modificación no autorizada puede repararse con facilidad o no afecta la operatoria normal.

1-Información cuya modificación puede repararse, pero ocasiona pérdidas leves.

2-Información cuya modificación no autorizada es de difícil reparación y ocasiona pérdidas significativas.

3-Información cuya modificación no autorizada no puede repararse y genera graves pérdidas.

DISPONIBILIDAD

0–Información cuya inaccesibilidad no afecta la operatoria de la Institución.

1–Información cuya inaccesibilidad continua hasta una semana podría ocasionar pérdidas significativas.

2-Información cuya inaccesibilidad continua por un periodo mayor a un día podría ocasionar pérdidas significativas.

3-Información cuya inaccesibilidad continua por más de dos horas podría ocasionar pérdidas significativas a la Institución.

Se asigna un valor por cada una de estas características y luego se tiene en cuenta el valor más alto. Dependiendo de esto la información quedará en una de las siguientes categorías:

❖ CRITICIDAD ALTA: alguno de los valores asignados es 3 (tres).

❖ CRITICIDAD MEDIA: alguno de los valores asignados es 2 (dos).

❖ CRITICIDAD BAJA: alguno de los valores asignados es 1 (uno).

4.4 **CONTROL DE ACCESOS**

4.4.a. Acceso a instalaciones.

Se deberán tomar las medidas necesarias para limitar el acceso físico a las instalaciones de procesamiento de información sólo a aquellas personas autorizadas, evitando así la libre circulación de personas extrañas a esta actividad.

4.4.b. Acceso a información crítica.

La institución adopta los mecanismos necesarios para garantizar que solo los usuarios autorizados accedan a los activos de información, utilizando una política de “mínimo privilegio”. Estos privilegios se otorgarán previa autorización de los niveles competentes y superiores de la organización, y deberán ser revisados periódicamente.

4.4.c. Acceso a la red de Internet-Wifi.

Se deberá disponer de dos redes en la Facultad. Una será de uso exclusivo de los usuarios internos, es decir, aquellas personas que forman parte del equipo de colaboradores de la institución. El acceso a la misma será concedido por un responsable autorizado del área de Sistemas. La segunda conexión estará a disposición de los estudiantes y visitantes. De este modo se evitará conexiones no seguras a la red por la que se manejan datos sensibles.

4.4.d. Acceso a servicios y aplicaciones.

Corresponde aplicar restricciones en los equipos de cómputo de modo que estén disponibles solo los sistemas y aplicaciones que sean realmente necesarios en cada caso para desempeñar las funciones de su cargo.

4.5 **SEGURIDAD FÍSICA Y AMBIENTAL.**

4.5.a. Política de escritorios limpios.

Implementar una política de escritorios limpios con el objetivo de reducir los accesos no autorizados a información crítica. Se busca proteger tanto los documentos que se encuentren en papel como en discos o dispositivos de almacenamiento extraíble. Los lineamientos generales son:

● Guardar en cajones o archivos bajo llave los documentos en papel o los dispositivos electrónicos en los que se almacene información cuando no estén siendo utilizados. Se aplica tanto en horario laboral como fuera de este.

● No dejar notas pegadas en los monitores con contraseñas o claves de acceso personales ni ajenas.

● Apagar y desconectar los equipos de impresión luego de terminar el horario laboral.

● Retirar las hojas impresas inmediatamente luego de que estén disponibles.

4.5.b. Seguridad de los equipos fuera de las instalaciones.

Los equipos de cómputo y almacenamiento, cualesquiera sean estos, propiedad de la Institución no pueden ser retirados de los recintos de la misma sin previa autorización del responsable del área.

En el caso de recibir dicha autorización se le debe hacer firmar un convenio bajo el cual asegure hacer uso responsable del elemento y aplicar las medidas de seguridad que sean necesarias.

4.5.c. Mantenimiento de Equipos.

El equipo de Sistemas de la Facultad será responsable de brindar el mantenimiento debido a los equipos según sus condiciones y necesidades particulares. En caso de no contar con las herramientas o el conocimiento para llevar a cabo esta tarea deberán asegurarse de tercerizar dicho servicio con un técnico cualificado que resguarde debidamente la información contenida en los aparatos.

4.5.d. Seguridad del cableado.

Los cables que distribuyen ya sea energía eléctrica o un servicio de comunicación y transporte de datos deben estar dispuestos de modo seguro para evitar ser dañado, interferido o afectado de cualquier otra acción de sabotaje.

4.6 **SEGURIDAD DE LAS COMUNICACIONES**

4.6.a. Protección de la información.

Toda la información que sea comunicada por la Institución debe ir acompañada de las medidas de protección necesarias para minimizar los riesgos que pudieran afectar y distorsionar el mensaje contenido en ella. La seguridad que se le aplique dependerá de su nivel de criticidad. Algunas técnicas que pueden ser utilizadas son las siguientes:

● Cifrado de información.

● Verificación de la integridad de la información por medio de Hash.

4.6.b Cuentas de correo corporativas.

Se deberá otorgar tanto al personal docente como no docente una cuenta institucional que deberán usar de manera obligatoria para el desempeño de sus tareas.

4.7 **SEGURIDAD OPERATIVA**

4.7.a. Seguridad en los procesos.

Los responsables de cada área de la Facultad deberán hacer un análisis de los riesgos a los que están expuestos en su departamento y aplicar los controles que sean necesarios. La comunicación de roles y responsabilidades debe ser clara y concisa, así como también las sanciones que se consideren oportunas ante conductas o comportamientos inapropiados.

4.7.b. Copia de seguridad.

En concordancia con la criticidad del proceso y de los activos intervinientes se deberá hacer un backup con la siguiente frecuencia:

❖ CRITICIDAD ALTA: realizar una copia cada una hora.

❖ CRITICIDAD MEDIA: realizar una copia por día.

❖ CRITICIDAD BAJA: realizar copia una vez por semana.

4.8 **GESTIÓN DE INCIDENTES**.

4.8.a. Evaluación y escaneo de vulnerabilidades.

La institución realizará monitoreo de los sistemas de información de manera periódica con el fin de prevenir, detectar y reportar posibles eventos de seguridad que puedan ocurrir en los diferentes activos de información. Se deberá comunicar debidamente estas vulnerabilidades con el fin de tomar las medidas correctivas en el menor tiempo posible.

4.8.b. Detección de eventos de seguridad.

Al detectarse un evento que pueda constituirse en un incidente de seguridad, se lo deberá comunicar de forma inmediata al área o autoridad competente. Si se produjo el incidente, y éste afectó a los activos de información, las autoridades procederán a comunicar el hecho de manera pública al resto de la organización y comenzar con un análisis de los daños ocasionados.

4.9 ASPECTOS DE SEGURIDAD PARA LA CONTINUIDAD DE LA GESTIÓN.

La Facultad contempla todos los aspectos de seguridad requeridos, especialmente cuando se trate de sistemas e información críticos. Se realizan análisis de probabilidad de ocurrencia e impacto a fin de determinar el riesgo posible, y se identificarán y calcularán los tiempos de recuperación requeridos en los procesos críticos.

4.10 CUMPLIMIENTO

La institución cumple las disposiciones legales, normativas y contractuales que le son aplicables, así como también el acatamiento de las políticas y normas de seguridad.

Se deberá atender y dar cumplimiento a las recomendaciones correspondientes a los distintos hallazgos producto de los controles y auditorías realizados, adoptando las medidas correctivas que correspondan.

CONCLUSIONES

La concientización de las personas que trabajan en esta institución educativa en cuanto a la importancia de seguridad de la información es de suma importancia debido a que los trabajadores de estos sectores estudiados constituyen la primera línea de defensa en la protección de la información de la organización. Al estar conscientes de los riesgos a los que están expuestos y las medidas que deben seguir, se convierten en activos clave para prevenir y mitigar amenazas. A su vez, ayuda a fomentar un cambio de comportamiento en los empleados. Al comprender los riesgos asociados con prácticas inseguras, como el uso de contraseñas débiles, hacer clic en enlaces sospechosos o compartir información confidencial, los trabajadores pueden adoptar medidas proactivas para proteger la información y evitar acciones que podrían poner en riesgo la seguridad de la institución.

Al empoderar a los empleados con conocimientos y habilidades en seguridad de la información, se fortalece la postura de seguridad general de la institución y se establece una cultura de seguridad sólida en todos los niveles.

Una política de seguridad de la información formalizada es esencial para una institución educativa superior, ya que proporciona una estructura sólida para proteger los datos sensibles, cumplir con las regulaciones, prevenir ataques cibernéticos, gestionar incidentes de seguridad y promover una cultura de seguridad. Al implementar y seguir esta política, la institución puede salvaguardar su reputación, garantizar la privacidad de sus miembros y mantener la continuidad de sus operaciones en un entorno digital cada vez más complejo y amenazante.

RECOMENDACIONES

Es esencial abordar adecuadamente los riesgos identificados en el área de cómputos. Se recomienda implementar medidas preventivas y de mitigación específicas para cada uno de los riesgos mencionados, como mejorar los sistemas de refrigeración, establecer protocolos de seguridad contra incendios, fortalecer las medidas de seguridad informática, implementar sistemas de seguridad física y considerar fuentes de energía alternativas. Estas acciones ayudarán a proteger la integridad, confidencialidad y disponibilidad de la información en la institución.

El sistema de gestión de alumnos que utiliza actualmente la facultad no es un sitio seguro. Es decir, que no cuenta con un certificado digital (o certificado SSL) que avale que las transacciones que se realizan por ese medio están protegidas y, a la vez, autentica la identidad del sitio web asegurando a los visitantes que no están ingresando a un sitio web falso. Se recomienda adquirir este certificado ya que allí se contiene información personal y sensible de los estudiantes como su legajo completo e historia académica, los cuales deben ser resguardados en cumplimiento de la Ley de Datos personales N° 25326.

Actualmente se hace un uso aproximado de tan solo el 15% de la capacidad de los servidores de la institución. Su funcionamiento 24/7 implica costos de mantenimiento y costos energéticos importantes que, además del punto de vista económico, tiene implicancias en el compromiso de la institución de perseguir la sustentabilidad en todas las actividades que realice. En cuanto a la economicidad y conveniencia del uso de servidores propios que posee la institución, es recomendable profundizar en el futuro un análisis con la alternativa de migrar a un servicio de cómputo en nube para el sistema de gestión de alumnos, el cual debería ser llevado convenientemente con las metodologías criptográficas que garanticen el nivel de seguridad acorde a la criticidad de la información que se estaría exteriorizando de las instalaciones propias. Una de las principales ventajas del cómputo en nube es la escalabilidad, es por esto que sería clave considerar desde un punto de vista cualitativo la presencia o no de cuellos de botella en la capacidad de procesamiento de los servidores actuales como punto de partida para el análisis futuro propuesto.

Bibliografía

- *Baca Urbina, G. (2016). Introducción a la Seguridad Informática. Grupo Editorial Patria.*

- *Controles de seguridad críticos de CIS (Versión 8, año 2021)*

- *Escrivá Gascó, G. Romero Serrano, R. Ramada, DJ. Onrubia Pérez, R. (2013). Seguridad Informática.1° edición. Macmillan Profesional.*

- *Hernández Sampieri, Roberto. Metodología de la investigación. Mcgraw hill education.*

- *IMB SkillsBuild for Students (s.f.). Fundamentos de ciberseguridad ¿Qué es la Ciberseguridad?*

- *INCIBE (s.f.). Glosario de términos de ciberseguridad: una guía de aproximación para el empresario.*

- *IRAM, Instituto Argentino de Normalización y Certificación (2013). Norma ISO/IEC 27001: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Subcomité de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad.*

- *IRAM, Instituto Argentino de Normalización y Certificación (2018). Norma ISO/IEC 27000: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Glosario. Subcomité de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad.*

- *IRAM, Instituto Argentino de Normalización y Certificación (2021). Norma ISO/IEC 27002: Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información. Subcomité de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad.*

- *Laudon & Laudon (2016). Sistemas de Información Gerencial.14º edición. Pearson.*

- *Marco de cumplimiento Cobit 2019: introducción y metodología.*

- *Matriz Mitre AT&CK.*

- *NIST (2019)- Marco de referencias en ciberseguridad - Edición 5.*

Apéndice

ENTREVISTA SECCIÓN ALUMNOS

1. ¿Con qué equipamiento de trabaja en el sector? ¿Qué programas utilizan para sus labores diarias?
2. ¿Existe alguna resolución por parte del rectorado en cuanto a la seguridad de la información que se sigue en la oficina?
3. ¿Los datos personales de los alumnos tienen algún tratamiento especial para su seguridad? ¿Pueden ser accedidos por todo el personal del área? ¿Se puede enviar la base de datos de alumnos por correo en caso de ser requerida?
4. ¿Existe algún tipo de clasificación de la información en base a su confidencialidad o privacidad?
5. ¿Se utilizan contraseñas individuales para cada usuario con acceso? ¿Existen contraseñas de grupos o genéricas?
6. ¿Se hacen firmar acuerdos de confidencialidad al personal que interviene en el sector?
7. ¿Qué tipos de usuarios tienen permiso de edición de los datos de la sección? ¿Existen alertas de modificaciones de datos? ¿Qué usuarios pueden hacer modificación de notas? ¿Las actas cerradas pueden ser modificadas? ¿Existe un registro de estas modificaciones?
8. ¿Existe un procedimiento en caso de incidentes de seguridad, como pérdida de datos o accesos no autorizados? ¿Se comunican estos incidentes?
9. ¿Se realizan capacitaciones sobre seguridad de la información y documental? ¿Se capacita a los colaboradores para reconocer ataques de ingeniería social? (Phishing, mensajes engañosos). ¿De ser afirmativo, que actividades realizan?
10. ¿Existen medidas de seguridad física ante accidentes? (incendios, cortocircuitos)
11. ¿Cuáles son las medidas de seguridad documental implementadas en la oficina para proteger la información? (Política de escritorios limpios)
12. ¿Todas las máquinas tienen antivirus? ¿Cuentan con acceso libre a internet?
13. ¿Tienen restricciones para la instalación de cualquier tipo de programa o software?

ENTREVISTA PARA SISTEMAS

1. ¿Tienen un inventario de activos de información? ¿Realizan una evaluación de riesgos sobre ellos?

2. ¿Se realizan frecuentemente escaneos de vulnerabilidades de los activos de información y de la red?
3. ¿La red de sistema de alumnos está segmentado respecto a la red de acceso público?
4. ¿En los servidores, se instalaron programas de seguridad como antivirus o firewalls?
5. ¿Existen cuentas de administrador para el acceso a activos o información sensible de la institución?
6. ¿Se realizan pruebas de penetración en los sistemas para medir la seguridad de los mismos?
7. ¿Se estableció una política de proceso de copia de seguridad (Backup)? ¿Con qué frecuencia se realiza? ¿Si se corrobora la integridad del back up? ¿Si se los almacena fuera del sitio? ¿Se realizan pruebas de restauración?
8. ¿Existe un control de cuentas de usuario?
9. ¿Existe un control de cuentas de correo electrónico? ¿Se dan de baja las cuentas cesantes?
10. ¿Se implementan medidas para prevenir el acceso no autorizado a la red y sistemas? ¿Se implementó autenticación de múltiples factores para acceso remoto?
11. ¿Se designó formalmente a una persona a cargo de la gestión de incidentes? ¿Qué cargo tiene en la organización?
12. ¿Cuál es el proceso para la disposición final segura de los dispositivos de almacenamiento y equipos electrónicos que contienen información sensible?
13. ¿En este departamento se tienen capacitaciones de seguridad o si brindan al personal de la FACE?

MODELO DE ENTREVISTA A PERSONAL DE CENTRO DE CÓMPUTOS

Aspectos generales

¿Cuántas personas trabajan en el área? ¿Cuál es la jerarquía entre ellas?
¿Con qué sectores de la institución mantienen relación directa?

Activos de información

¿Cuáles son los activos con los que se cuenta? ¿Cuántos son considerados críticos, o los más importantes, en la institución?
¿Se mantiene un inventario de activos de información? En el caso de respuesta afirmativa ¿Con qué periodicidad se revisa?
¿Se clasificó a los activos de información en términos de confidencialidad, integridad y disponibilidad?
¿Con qué frecuencia se escanea los activos en busca de vulnerabilidades?
¿Cuál es la rapidez con la que se abordan las vulnerabilidades detectadas?

Control de accesos

¿Se mantiene un control de acceso físico sobre las instalaciones de procesamiento y manejo de la información?
¿Hay un control sobre el número de usuarios que tienen acceso a la información confidencial?

Herramientas de seguridad de la información

¿Existe una política de contraseñas seguras y no compartidas para el acceso a los sistemas de información?
¿Se cuenta en el área con programas de seguridad para los activos instalados en los sistemas?

Seguridad de la información

¿Existe una política de seguridad de la información?

¿Cuáles considera son los puntos débiles en cuanto a la seguridad de la información según las medidas que se toman actualmente?
¿Se tratan temas de seguridad de la información en los diferentes niveles jerárquicos de la institución?
¿Se ha designado un responsable que pueda conducir a la organización para el cumplimiento de los temas relacionados con la Seguridad de activos de información y otros de su organización?

MODELO DE FICHA DE OBSERVACIÓN

1. Artefactos
¿Con qué tipos de equipos de cómputo cuenta el área? ¿Cuáles son sus características? (Especificar cuántos son)
¿Cómo están archivados los documentos físicos que se manipulan en el sector?
¿De qué tipo es el soporte donde se resguardan los datos en formato digital?
¿Se cuenta con sistemas de gestión computarizados?
¿Con qué otros recursos tecnológicos se cuentan?
¿Cuál es el medio de conexión que se utiliza? (cable de fibra, línea telefónica, inalámbrica, etc)

2. Acceso
¿El sector está ubicado en un área muy transitada?

¿Con qué sistema de seguridad se controla el acceso físico a la oficina?

3. Aspectos generales de la oficina
¿De qué manera se distribuyen los escritorios?
¿Cuál es el nivel de iluminación? (natural o artificial)
¿Existen tableros informativos con medidas de seguridad?
¿Cuál es el método de refrigeración que se utiliza?