Universidad Nacional de Tucumán
Facultad de Ciencias Económicas
Asignatura: “Seguridad y Control en Sistemas Informáticos”

ELABORACIÓN DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA UNA INSTITUCIÓN EDUCATIVA DE NIVEL SUPERIOR

ESPER, Facundo Augusto
HILZINGER, Nicolás Eduardo
SALICA, Agustina Denisse

2022

Declaración jurada del origen de los contenidos

"Por medio de la presente, los autores manifiestan conocer y aceptar el "Reglamento para la Presentación de Trabajo Final" vigente de la asignatura "Seguridad y Control en Sistemas Informáticos", haciéndose responsables por la totalidad de los contenidos del presente documento, los cuales son originales y de creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación nacional e internacional de Propiedad Intelectual".

ESPER, Facundo Augusto. "FIRMADO"
HILZINGER, Nicolás Eduardo. "FIRMADO"
SALICA, Agustina Denisse. "FIRMADO"

TABLA DE CONTENIDOS

ELABORACIÓN DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA UNA INSTITUCIÓN EDUCATIVA DE NIVEL SUPERIOR

Esper, Facundo Augusto – Hilzinger, Nicolás Eduardo –Salica, Agustina Denisse
Universidad Nacional de Tucumán – Facultad de Ciencias Económicas
- facuuesper@gmail.com - nicolashilzinger@gmail.com - agustinasalica1274@gmail.com -

1. RESUMEN

En el presente trabajo se pretende abordar la creación de una política de seguridad de la información destinada a una institución educativa de nivel superior, como lo es una de las Facultades de la Universidad Nacional de Tucumán. Durante el mismo, se realizará un análisis de los diferentes activos de información con los que cuenta dicha institución, valorando su criticidad, riesgo e importancia, entre otras características, con el fin de asegurar la aplicación y cumplimiento de los tres pilares de la seguridad de la información que son la confidencialidad, la integridad y la disponibilidad de estos activos de información.

Este trabajo se abordará desde un enfoque cualitativo, en donde se utilizará tanto la observación directa como entrevistas a personas clave en la institución para la recolección de datos.

Palabras Clave: Políticas - Seguridad - Activos de información - Riesgos.

2. INTRODUCCIÓN

Con el pasar de los años, la seguridad de la información se fue convirtiendo en una disciplina cada vez más importante en todo tipo de organizaciones, tanto en aquellas con fines de lucro como en aquellas en donde el objetivo principal no es la persecución de un rédito económico.

La acelerada globalización y la creciente aparición de nuevas y disruptivas tecnologías, y por consiguiente, la falta de medidas de seguridad, trajo consigo el surgimiento de ciber-atacantes que se aprovechan de estas vulnerabilidades en las organizaciones para robar información crítica y extorsionar a estas empresas.
En los últimos años, y en especial durante la pandemia del COVID19, los incidentes informáticos se incrementaron de manera exponencial generando grandes pérdidas económicas y de imagen en todo tipo de organizaciones. Estos incidentes se produjeron tanto por errores humanos de los propios miembros de las organizaciones como por ataques externos.

Un informe del Equipo de Respuesta ante Emergencias Informáticas de Argentina (CERT, por su sigla en inglés. - https://www.argentina.gob.ar/ febrero de 2022 -) registró durante el año 2021 un incremento de incidentes informáticos del

261% con respecto al año 2020, donde el phishing y el ransomware se ubican como los tipos de incidentes más reportados.

En vista de lo antes mencionado es indispensable contar con medidas de protección preventivas y reactivas para hacer frente a los desafíos que se presentan al recolectar, almacenar y gestionar la información en las organizaciones.

Es especialmente necesario instaurar dichas salvaguardas en organismos como el que es base de nuestro estudio, un centro de educación de nivel superior público, en donde la ausencia de una política de seguridad de la información podría representar una gran vulnerabilidad.

Surgen entonces las siguientes preguntas que guiarán el desarrollo del presente trabajo:

- ¿Cuáles son los aspectos y procedimientos de seguridad de la información aplicadas por la organización?
- ¿Cuáles son las situaciones que podrían significar un riesgo y cuál sería su impacto en el desarrollo de las actividades?
- ¿Cómo podría diseñarse una política de seguridad de información aplicable a la institución?

OBJETIVOS

Objetivo general:

Recomendar un modelo de política de seguridad de la información en donde se contengan los primeros lineamientos que guíen la acción en este campo.

Objetivos Específicos:

- Identificar qué aspectos y procedimientos de seguridad de la información son abordados por la organización.
- Evaluar cuales son las situaciones riesgosas a las que se expone al desarrollar sus actividades y cuál podría ser el impacto en su funcionamiento.
- Proponer una política de seguridad de la información.

A partir de los objetivos , se desarrolla el marco teórico.

3. MARCO TEÓRICO

Seguridad de la información

Según Baca Urbina G.(2016) la Seguridad de la información es un conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información:

- Integridad: garantizando que tanto la información como sus métodos de proceso son exactos y completos.

- Confidencialidad: asegurando que únicamente pueden acceder a la información y modificarla los usuarios autorizados.
- Disponibilidad: permitiendo que la información esté disponible cuando los usuarios la necesiten.

Este término, por tanto, es un concepto amplio que engloba medidas de seguridad que afectan a la información independientemente del tipo de esta, soporte en el que se almacene, forma en que se transmita, etc.

Incidente de Seguridad

INCIBE en su glosario (2020) explica que un Incidente de Seguridad es cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

Activo de Información

Laudon & Laudon (2016) considera que 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.

Amenaza

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.

Vulnerabilidad

Según Escrivá Gascó, G. Romero Serrano, R. Ramada, DJ. Onrubia Pérez, R. (2013) una vulnerabilidad representa la debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos. Constituye un hecho o una actividad que permite concretar una amenaza. Se es vulnerable en la medida en que no hay suficiente protección como para evitar que llegue a suceder una amenaza.

Impacto

INCIBE (2020) declara que el impacto generado sobre un activo de información es la consecuencia de la materialización de una amenaza. Los hay de distintos tipos: imagen, compliance, negocios y activos.

Probabilidad

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

Riesgo

Escrivá Gascó, G. Romero Serrano, R. Ramada, DJ. Onrubia Pérez, R. (2013) establecen que 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

"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 (INCIBE,2020).

Ciberataque

Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema (INCIBE, 2020).

Ciberdelincuente

Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de software o hardware, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos (INCIBE,2020).

Ransomware

Escrivá Gascó, G. Romero Serrano, R. Ramada, DJ. Onrubia Pérez, R. (2013) explican que este término "proviene de la unión de las palabras inglesas ransom (rescate) y software. Este tipo de malware cifra archivos importantes del disco duro para exigir el pago de dinero a cambio de la contraseña para descifrarlos".

Phishing

Según Baca Urbina, G. (2016) el phishing es una técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esas personas.

Los ciberdelincuentes envían correos electrónicos falsos como anzuelo para “pescar” contraseñas y datos personales valiosos.

Ingeniería social

Laudon & Laudon (2016) establece que 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.

Política de Seguridad de la Información

INCIBE (2020) describe la Política de Seguridad de la Información (PSI) como un documento central para la protección de los datos y de los recursos utilizados para su tratamiento, que define la postura de una organización respecto al comportamiento que espera de empleados, autoridades y terceros que tomen contacto con dichos datos y/o recursos, para su protección.

A partir del marco teórico, se desarrolla el marco metodológico:

4. MARCO METODOLÓGICO

La unidad de análisis es un centro de educación de nivel superior ubicado en la Provincia de Tucumán.

Este trabajo de investigación se realizará mediante un enfoque cualitativo, ya que se pretende comprender las distintas percepciones sobre una situación particular. El diseño será de investigación-acción, debido a que primero analizaremos la situación en que se encuentra la organización, para luego proponer una política que se ajuste a los problemas encontrados mediante este análisis.

Utilizaremos las siguientes herramientas para la recolección de datos:

- Observación con participación pasiva sobre:
  1) Actividades individuales y colectivas: para identificar qué procesos se llevan a cabo y de qué manera se realizan.
  2) Artefactos: para relevar qué activos de información se utilizan.
- Entrevistas a expertos: especialmente al personal encargado de la institución.

5. SOBRE EL CENTRO DE EDUCACIÓN DE NIVEL 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. Se forma entonces una comisión a la que se le confía la responsabilidad de conseguir el aval de las autoridades nacionales para la fundación de este centro educativo, y luego de extensas gestiones se logra con el objetivo.

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.

6. RESULTADOS

6.1 Observación

- Actividades individuales y colectivas: El personal que trabaja en el área de Sistema tiene una jornada laboral de cuatro horas diarias, de lunes a viernes. Atienden mediante una plataforma informática y en casos

especiales por vía telefónica. La oficina se encuentra en un sector de poco tránsito y a la que solo pueden acceder quienes pertenecen a esta sección. No tienen un uniforme definido pero visten de manera formal. En cuanto al ambiente laboral prevalece el espíritu colaborativo y amigable.

- Artefactos: en una de las secciones de la oficina se encuentra una sala bajo llave en donde se resguarda el servidor físico que contiene la base de datos más crítica además de dos dispositivos de almacenamiento con discos redundantes, switchs y routers. En este mismo lugar hay un estante que contiene piezas de repuesto para el servidor y otros aparatos que han quedado en desuso luego del proceso de modernización que se llevó a cabo recientemente. A su vez, cada colaborador cuenta con su computadora de escritorio.

6.2 Resultados obtenidos en la Entrevista.

La Dirección de Sistemas de la Facultad depende de la Secretaría Administrativa y está compuesto de dos sectores:

- Desarrollo.
- Tecnología y Seguridad.

Se realizó una entrevista al Ingeniero a cargo del área mencionada en segundo lugar, el cual detalló cómo aborda la organización los procesos y actividades referidos a la Seguridad de la Información.

De manera general, las tareas que se realizan allí están orientadas a dar soporte técnico para el manejo físico de los equipos de cómputo y los sistemas de gestión utilizados en ellos buscando un uso consciente y seguro de los mismos.

Actualmente se cuenta con un sistema a través del cual se cargan los "tickets", que es como denominan a las solicitudes particulares o informes de inconvenientes, en donde se registran y clasifican las consultas para dar prioridad a los asuntos de mayor urgencia. A su vez, permite de manera simultánea que el usuario pueda hacer un seguimiento de su "ticket". El acceso al mencionado sistema se encuentra restringido de modo que solo pueden acceder los miembros de la plantilla de trabajadores dependientes de la Facultad. Los mismos son registrados por el técnico haciendo uso del email corporativo de cada persona.

Gracias a esto resulta factible hacer un seguimiento del desempeño del sector, ya que, el programa arroja información acerca de cómo se brinda soporte al sector administrativo y al resto de áreas del centro educativo, indicando cuáles son los tiempos de respuesta, entre otros datos, con los que es posible armar informes y estadísticas para mejorar la gestión. Aunque la realidad marca que en el día a día no son utilizados para tal fin.

<u>Herramientas y Técnicas de Seguridad de la Información identificadas.</u>

1) **Inventario de activos de información:** La institución posee una sección denominada *"Bienes del Estado"* , que depende directamente de la secretaría de administración, la cual realiza dicho inventario en donde especifica quien es el responsable de cada bien y cual es el código único de identificación que le pertenece.
   Algunos de los activos que se identifican son los siguientes:

- Base de datos del sistema de gestión de alumnos: al usarse un sistema antiguo se encuentra en un motor de base de datos Informix ubicado en servidores físicos en el departamento de Sistemas.
- Servidor físico.
- Servicio de nube de google: donde se almacenan los mails.
- Switch
- Router.
- Access point.
- Storage

2) **Escaneo de vulnerabilidades:** De manera periódica se escanea tanto el sitio de gestión de alumnos como las computadoras de toda la organización en busca de vulnerabilidades.
3) **Segmentación de redes:** Internamente se aplican VPN "Virtual Private Network" (Red Privada Virtual) distintas para que la conexión WI-FI utilizada en los servidores y equipos de trabajo estén separados de la que está disponible para uso común de los estudiantes y demás visitantes. Se les aplicó un proceso de endurecimiento (hardening) con el objetivo de reducir los peligros y amenazas.
4) **Protección de información en formato papel:** La documentación confidencial que necesariamente se encuentra contenida en formato papel se resguarda bajo llave en las oficinas correspondientes.
5) Controles de acceso físico: específicamente en el área de Sistemas, donde se resguarda información sensible, sólo puede ingresar personal autorizado. Además la sala en donde se encuentra alojado el servidor físico con las bases de datos más críticas está permanentemente cerrada como medida de seguridad. Aun así se tiene conciencia de la necesidad de aumentar el nivel de seguridad en estas zonas de trabajo.
6) **Seguridad ambiental:** Se cuenta con matafuegos especiales para que en caso de ser necesario utilizarlos no dañen los dispositivos electrónicos. También existe un sistema de refrigeración especial en la sala de servidores.
7) Esquema de Backup: Existen dos tipos de guardado que se detallan a continuación.

- A nivel de servidor se realiza una copia diaria antes del inicio de actividades generalmente a las cinco o seis de la mañana.
- A nivel base de datos la copia sigue un modelo incremental.
  Disponen de dos storage (dispositivo central de almacenamiento) con redundancia de cinco discos en donde se respaldan los datos.

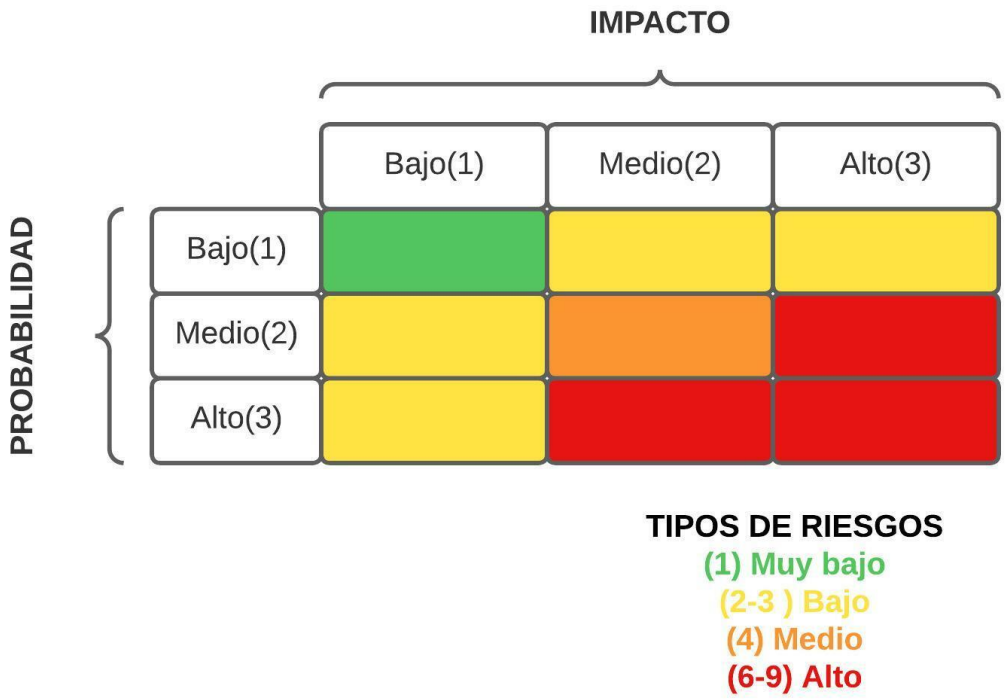
Título: Nube de palabras con resultados de la entrevista.

Fuente: Elaboración propia (usando https://www.nubedepalabras.es/).

ANÁLISIS DE RIESGOS

Teniendo en cuenta que el riesgo es el producto del impacto por la probabilidad de ocurrencia se fija la siguiente matriz de clasificación con su respectiva explicación.

Título: Matriz de clasificación de riesgos.



Fuente: Elaboración propia.

Esta matriz es una herramienta muy útil cuando se realiza un análisis de evaluación de riesgo ya que permite clasificar a éstos según su criticidad y su probabilidad de manifestarse en un incidente grave de seguridad. Dicha herramienta permite a los responsables de la organización actuar con mayor inmediatez frente a aquellos riesgos clasificados como altos y tomar las medidas correctivas que se consideren adecuadas para mitigar este riesgo.

Realizando un análisis en la institución bajo estudio, podemos destacar los principales riesgos y su clasificación de acuerdo a la matriz ya mencionada:

1. Temperaturas elevadas 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 se puede ver gravemente afectado de generarse una temperatura muy elevada. A causa de que los servidores se encuentran funcionando 24/7 es muy posible que en algún momento se presente un aumento de temperatura en los equipos que pueda generar graves inconvenientes. Por esto es que se asigna la clasificación máxima de riesgo (probabilidad alta, impacto alto).
2. Riesgo de incendios. Es uno de los principales riesgos naturales que surgen en todo tipo de organizaciones. 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.

Según el análisis, clasificamos este riesgo con una probabilidad de ocurrencia media y un impacto resultante alto.

3. Riesgo de sufrir 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, por medio de alguna criptomoneda y dentro de un límite establecido de tiempo. Una de las formas de dar ingreso al ransomware es mediante el phishing, que es un tipo de ataque derivado de la ingeniería social que consiste en el engaño, a través de emails y páginas web falsas que aparentan ser auténticas. 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 1: Análisis de Riesgo.

Ranking	Detalle del Riesgo	Probabilidad de ocurrencia	Impacto	Tipo de riesgo
1	Fallos en servidor por alta temperatura.	Alta(3)	Alto(3)	Alto(9)
2	Riesgo de incendios.	Media(2)	Alto(3)	Alto(6)
3	Riesgo de malware	Media(2)	Alto(3)	Alto(6)
4	Robos de equipos.	Media(2)	Medio(2)	Medio(4)
5	Cortes de energía eléctrica.	Alta(3)	Bajo(1)	Bajo(3)

Fuente: Elaboración propia.

PROPUESTA

Luego de evaluar la situación actual del centro de educación de nivel superior se recomienda la elaboración e implementación de la siguiente Política de Seguridad de la Información, la cual toma como base la Disposición 01/2022 emitida por el Director Nacional de Ciberseguridad de la Jefatura de Gabinete de Ministros Dirección Nacional de Ciberseguridad que contiene un "Modelo referencial de Política de Seguridad de la Información" aplicable a entidades comprendidas en el art. 8º de la Ley 24.156.

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

4.1ORGANIZACIÓN 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).

Tabla 2: Clasificación de la Información.

CRITICIDAD ALTA	CRITICIDAD MEDIA	CRITICIDAD BAJA
3	2	1

Fuente: Elaboración propia.

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 monitoreos 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.

7. CONCLUSIONES

Las organizaciones, cualquiera sea su tipo, están empezando a reconocer la importancia de implementar medidas de seguridad para proteger sus activos de información. Se realizan grandes esfuerzos en busca de asegurar su integridad, disponibilidad y confidencialidad teniendo plena conciencia de que estos representan el corazón de las operaciones que allí se realicen.

La tarea de tener bajo control los sistemas de captura, procesamiento y almacenamiento de datos en formato papel o electrónico no es sencilla.
Dependiendo de la situación particular de cada Institución, el personal que posea, los recursos que tenga a disposición, entre otros factores, estará expuesta a una gran diversidad de riesgos que van evolucionando de la mano con los cambios tecnológicos y sociales que se desarrollan en todo el mundo.

A lo largo del presente trabajo de investigación se desarrolló una mirada orientada a la aplicación práctica, en el día a día, de los conocimientos incorporados de la asignatura “Seguridad y Control en Sistemas Informáticos”, la cual se procuró materializar en el contenido del mismo.

Se destaca que la institución analizada muestra una actitud progresista en lo que respecta a la mejora de la Seguridad de la Información, el personal se preocupa por adecuarse al entorno en constante movimiento en el que está inserto, por medio de la capacitación constante. Si bien el sistema tiene sus falencias, se tiene conciencia de los puntos débiles y se busca brindar las soluciones pertinentes a la brevedad.

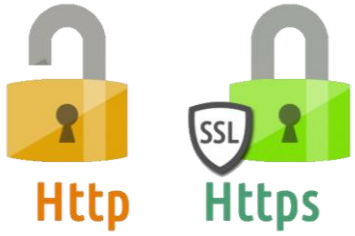
Por último, se espera que las políticas aquí presentadas, así como las recomendaciones propuestas, sean de utilidad como punto de partida para aplicaciones futuras en materia de Seguridad de la Información de esta y otras Facultades miembros de la Universidad Nacional de Tucumán, y para cualquier institución de nivel superior ubicada en el territorio nacional.

8. RECOMENDACIONES

- 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.

Título: Certificado Digital.



Fuente: Google Images.

- Considerando los riesgos a los que está expuesta la sala en donde se alojan los servidores físicos se propone actuar preventivamente para evitar siniestros adquiriendo un sensor con alarma que no solo marque la temperatura, como el dispositivo que poseen en la actualidad, sino que también pueda alertar cuando se supere una determinada cantidad de grados. Además sería muy conveniente sumarle un detector de humo ya que al estar tan sellada el área, los días o los horarios en donde no se trabaja pudiera gestarse un incendio y nadie se enteraría hasta que fuera demasiado tarde.
- 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. Desde el punto de vista ambiental, se recomienda profundizar en la posibilidad de incorporar formas de obtención de energías renovables, como pueden ser paneles solares, por ejemplo. 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.
- Se propone la implementación de programas de capacitación en lo que refiere a técnicas de ingeniería social para mantener al personal de la institución bien informado y alerta, y evitar de esta manera ser víctima de una de estas técnicas que se encuentran cada vez más presentes en todo tipo de organizaciones.

- Con respecto a la redundancia, si bien se cuenta con discos RAID que otorgan protección ante una eventual falla, las copias de seguridad son alojadas en el mismo centro de servidores por lo que se podrían ver expuestos a las mismas eventualidades que pudiera llegar a sufrir el soporte de datos central, como desastres naturales (incendios, inundaciones, terremotos, etc) y aquellos siniestros como robos o sabotaje. Lo recomendable es que los activos de información redundantes sean almacenados en un lugar distinto al del principal, para que este "respaldo" se encuentre realmente protegido y cumpla con su propósito.
- Con el fin de continuar con la incorporación de nuevas y funcionales tecnologías que permitan incrementar la seguridad de los diferentes activos de información, se propone comenzar con el proceso de implementación de la firma digital. Este sistema colaborará con el cumplimiento de otras características de la seguridad de la información como ser autenticación y no repudio.

9. REFERENCIAS BIBLIOGRÁFICAS

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

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

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

INCIBE. (2020). *Glosario de términos de ciberseguridad - Una guía de Aproximación para el empresario.*

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

INCIBE(s.f.). *Protección de la información*. Colección: Protege tu empresa. (https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf)

NIST (2019)- *Marco de referencias en ciberseguridad* - Edición 5. (https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf)

CERT(2022) *Informe anual CERT*. (https://www.argentina.gob.ar/noticias/se-publico-el-informe-anual-del-

certar)

Dirección Nacional de Ciberseguridad. Jefatura de Gabinete de Ministros. (2022). *Modelo Referencial de Política de Seguridad de la Información. Disposición 01/2022*. CABA

10. APÉNDICE

MODELO DE ENTREVISTA A EXPERTOS

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? ¿Cuantos 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?