Identificación y Análisis de Controles de Seguridad de la Información en una Institución de Educación Universitaria

Mª Alejandra Masclef[1y4], Marcelo Adrián García[2y4], Claudia Scro[3y4]

[4]Instituto de Administración de la Facultad de Ciencias Económicas de la Universidad Nacional de Tucumán, San Miguel de Tucumán, T T4002BLS

[1]alema@webmail.unt.edu.ar,[2]mgarcia@face.unt.edu.ar,[3]cscro@face.unt.edu.ar

Resumen. El objetivo general de este trabajo es identificar los controles de seguridad de la información aplicables en la Dirección Alumnos de la Facultad de Ciencias Económicas de la Universidad Nacional de Tucumán (UNT). En el desarrollo se tienen en cuenta las buenas prácticas propuestas por "Center for Internet Security" (CIS) y el anexo "A" de la norma ISO 27001 Sistema de Gestión de Seguridad de la Información. A partir de estas, se efectúa un análisis de los controles de seguridad y se determina un nivel de madurez centrado en controles organizacionales, de personas y físicos (ambientales y documentales). Se aborda este trabajo desde un enfoque cualitativo, con un diseño de investigación - acción. Las técnicas utilizadas para la recolección de los datos son la revisión de marcos de cumplimiento, las entrevistas y la observación directa y participante activa. Como resultado, se presentan los principales hallazgos y recomendaciones para lograr fortalecer el entorno de seguridad física, ambiental y documental del sector objeto de estudio. El trabajo se desarrolla en el marco del Proyecto PROMCE – PICE 2022 N° CU54-UNT2652, "Análisis del nivel de madurez de seguridad de la información en procesos críticos de una institución de educación superior", aprobado según Resolución 539 HCD 22.

Palabras clave: Seguridad de la Información, Controles, Madurez, Institución de Educación Superior

1 Introducción

Los activos de información otorgan valor a las organizaciones, por lo que deben ser resguardados de los riesgos a los que están expuestos. En este contexto cobra significativa importancia la seguridad de la información (SI), que propicia la protección de las características de integridad, disponibilidad y confidencialidad ante cualquier tipo de amenaza. Un incidente dificultaría el normal desenvolvimiento de las actividades de la organización o podría generar un impacto reputacional o de cumplimiento normativo.

Considerando que el objeto de estudio del presente es la Dirección Alumnos de una institución de educación superior y teniendo en cuenta sus procesos críticos en los que

intervienen datos personales e información académica de sus alumnos, resulta indispensable el resguardo de las mencionadas características de la información a través de la aplicación de adecuados controles sobre sus activos informáticos.

El presente trabajo se desarrolla en el marco del Proyecto PROMCE – PICE 2022 N° CU54-UNT2652, "Análisis del nivel de madurez de seguridad de la información en procesos críticos de una institución de educación superior", aprobado según Resolución 539 HCD 22. El objetivo general del proyecto es identificar los controles aplicables al sector, analizarlos y establecer un nivel de madurez de seguridad de la información en base a estándares internacionales. Como resultado se describirán los principales hallazgos con la finalidad de dar a conocer la situación y se desarrollarán recomendaciones que tiendan al fortalecimiento de la seguridad de la información en el sector.

2 Planteamiento de Objetivos

El objetivo general de este trabajo es identificar los controles de seguridad de la información aplicables al sector objeto de estudio, teniendo en cuenta las buenas prácticas propuestas por CIS y el anexo "A" de la norma ISO 27001.

A partir de ello, se persigue:

- Analizar los controles anteriormente descriptos,
- Establecer un nivel de madurez enfatizando en controles organizacionales, de personas y físicos (ambientales y documentales).

3 Marco Teórico

Según lo establece ISO/IEC 27000 (2018), la seguridad de la información garantiza las características de confidencialidad, disponibilidad e integridad de la información. A tal fin, involucra la aplicación y gestión de controles apropiados que implican la consideración de una amplia gama de amenazas, con el objetivo de garantizar el éxito y la continuidad de las actividades habituales de la organización, minimizando las consecuencias que podría ocasionar un incidente.

Este conjunto de controles se selecciona a través de un proceso de evaluación de riesgos. Estos controles deben especificarse, implementarse, monitorearse, revisarse y mejorarse cuando sea necesario, para garantizar que se cumplan los objetivos de la institución y los de la seguridad de la información en particular. Posteriormente a su implementación se deben gestionar adecuadamente a través de políticas, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de información identificados.

El Instituto Nacional de Ciberseguridad de España – INCIBE -, en el glosario de términos de ciberseguridad, define a los activos de información como:

> 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. (s.f., p.12)

La información constituye un activo valioso y vulnerable. Su destrucción, modificación, divulgación o acceso no autorizado puede comprometerla total o parcialmente, causando retrasos y contingencias no previstas. Es por ello que la seguridad de la información ha tomado relevancia en el ámbito de las Ciencias Económicas. Con el creciente atravesamiento de la tecnología y la información en los procesos de negocio, es fundamental asegurar que se encuentre protegida. Su adecuado resguardo y la mitigación de los riesgos asociados a su captación, manipulación, almacenamiento y salida, son aspectos importantes para garantizar su confidencialidad, integridad y disponibilidad. Además, ello permite cumplir con las regulaciones y normativas vigentes.

El glosario de ciberseguridad de INCIBE, define riesgo de la siguiente manera:

> Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado. El riesgo puede ser mitigado mediante políticas de seguridad y continuidad del negocio que suelen prever posibles ataques y proponen soluciones de actuación ante situaciones cuyo riesgo pueda ser elevado. (s.f., p.67)

La misma institución define evaluación de riesgos:

> Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a las 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. (s.f., p. 14)

Como referencia, se abordan dos marcos de cumplimiento vinculados a la temática aquí desarrollada: CIS e ISO 27001.

Los controles de seguridad de la información de CIS Security (2021), por su sigla en inglés “Critical Security Controls”, en su versión 8 indica que son un conjunto de medidas y prácticas recomendadas para proteger los activos de información y fortalecer la postura de seguridad de una organización. Estos controles cubren una amplia gama de áreas críticas de seguridad y están destinados a abordar los desafíos actuales en el panorama de amenazas informáticas.

Al seguir estos controles y llevar adelante sus recomendaciones, se puede medir su cumplimiento y el nivel de implementación de los controles en cada dominio, los mismos se detallan a continuación:

1. Inventario y control de activos empresariales
2. Inventario y control de activos de software
3. Protección de datos
4. Configuración segura de activos y software empresariales

5. Administración de cuentas
6. Gestión de control de acceso
7. Gestión continua de vulnerabilidades
8. Gestión de registros de auditoría
9. Protecciones de correo electrónico y navegador web
10. Defensas contra malware
11. Recuperación de datos
12. Gestión de infraestructura de red
13. Monitoreo y defensa de redes
14. Concientización sobre seguridad y capacitación en habilidades
15. Gestión de proveedores de servicios
16. Seguridad del software de aplicación
17. Gestión de respuesta a incidentes
18. Pruebas de penetración

La norma ISO 27001 (2022) detalla los requisitos para implementar un sistema de gestión de la seguridad de la información, en su anexo "A" especifica controles clasificados en cuatro tipos: organizacionales, de personas, físicos y tecnológicos.

Una de las cualidades de la utilización de estos marcos de cumplimiento es su capacidad para evaluar el estado de madurez de seguridad de la información.

Un modelo de seguridad de la información busca establecer una valoración estandarizada con la que se pueda determinar el estado de la seguridad de la información en una organización, permitiendo determinar planes de acción para alcanzar las metas de seguridad deseadas.

Fortalecer el nivel de madurez no es una iniciativa a corto plazo, la mayoría de las corporaciones necesitan al menos un par de años para pasar de la fase inicial a la finalización de la fase optimizada. La evaluación periódica del programa es importante para seguir el progreso y comunicar los avances a las partes interesadas. También deben tenerse en cuenta el tiempo y los recursos insumidos en cada fase. En muchos casos, el costo y el esfuerzo de implementar controles para alcanzar los tramos superiores del modelo superan los beneficios incrementales.

4 Aspectos Metodológicos

Se aborda este trabajo desde un enfoque cualitativo, con un diseño de investigación - acción. Las técnicas utilizadas para la recolección de los datos son la revisión de marcos de cumplimiento, las entrevistas y la observación directa y participante activa.

5 Resultados y Discusión

5.1 Generalidades

La Dirección Alumnos de la Facultad de Ciencias Económicas, gestiona una gran cantidad de información valiosa, confidencial y sensible. Su pérdida, divulgación,

modificación o brecha de seguridad podría ocasionar consecuencias graves, como la violación de la privacidad, la interrupción de las operaciones, el perjuicio a los propietarios de los datos, el impacto en la reputación, entre otros. Además, se debe tener en cuenta que la organización está sujeta a regulaciones y normativas específicas, como la Ley de Protección de Datos Personales.

En el desarrollo del cronograma del trabajo previsto, se ha realizado el estudio exhaustivo de los marcos de cumplimiento anteriormente mencionados y la revisión documental. Asimismo, se llevó a cabo la observación directa y participante activa. Además, se realizaron entrevistas a la Directora y la Coordinadora del área.

Teniendo en cuenta las buenas prácticas de "CIS Control" y los controles del Anexo "A" de la norma ISO 27001, se presentan los principales hallazgos y recomendaciones a fin de fortalecer el entorno de seguridad física, ambiental y documental del sector objeto de estudio.

Conforme lo establece la norma ISO 31000 (2018) de Gestión del Riesgo, dicha gestión implica dos etapas: evaluación y tratamiento. En esta última, las acciones posibles son: aceptación, reducción, transferencia y evitación.

A través de las entrevistas, se identificaron los principales riesgos del sector. A partir de esto, se seleccionaron los controles considerados adecuados para el tratamiento de estos.

De un total de 93 controles analizados, 43 se consideraron aplicables teniendo en cuenta las características particulares y los datos gestionados por el área. La información obtenida de los instrumentos metodológicos aplicados se organizó y sistematizó en una matriz que nos permitió evaluar el grado de implementación de cada uno de ellos.

En la siguiente tabla se muestra cada tipo de control con el nivel de madurez determinado:

Table 1. Distribución de controles según nivel de madurez

Capitulo	Nivel de Madurez						
	N/A - No Aplica	0 - Inexistente	1 - Inicial	2 - Gestionado	3 - Definido	4 - Cuantitativo	5 - Optimizado
Controles Organizativos	15	7	3	10	2	0	0
Controles de Personas	1	3	3	0	1	0	0
Controles Fisicos	3	2	3	5	1	0	0
Controles Tecnológicos	31	1	0	1	1	0	0
	50	**13**	**9**	**16**	**5**	**0**	**0**

Nota: Elaboración propia en base al modelo CMMI.

Los niveles de madurez se definen de la siguiente manera:

- **0. Inexistente**: no se realiza ninguna actividad al respecto.
- **1. Inicial**: estado donde el éxito de las actividades se basa, la mayoría de las veces, en el esfuerzo personal. Los procesos son desorganizados, totalmente reactivos y los roles y responsabilidades están mal o poco definidos.

- **2. Gestionado**: se aplican las buenas prácticas en base a la experiencia. Están definidos informalmente los procesos a realizar y los hitos para su revisión. Las definiciones no aplican a nivel corporativo ni existe normalización.
- **3. Definido**: la organización participa en el proceso. Existen métodos y templetes definidos y documentados. Existen normativas y procedimientos aprobados que regulan la actividad. Los correspondientes actores han sido formados.
- **4. Cuantitativo**: se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos.
- **5. Optimizado**: en base a criterios cuantitativos, se pueden determinar las desviaciones más comunes y optimizar los procesos. En lo sucesivo, se reducirán costos debido a la disminución de problemas y a la continua revisión de los procesos.

Fig. 1. Niveles del modelo CMMI

Nota: Elaboración propia en base al modelo CMMI

Como se detalla a continuación, estos controles fueron clasificados en tres grupos: organizativos, de personas y físicos. Cabe aclarar, que debido a que solo había tres controles tecnológicos aplicables, esta clasificación no fue considerada en el presente, a efectos de no producir una distorsión en los porcentajes de madurez.

En primer lugar, se ponen de manifiesto las fortalezas detectadas en el sector analizado: los referentes del área tienen identificados los requisitos legales, estatutarios, reglamentarios y contractuales aplicables. Además, manifiestan que el sector tiene revisiones independientes periódicas por parte del Rectorado de la UNT. A todo el personal de la institución se le realiza una verificación de antecedentes de manera previa a su

contratación. Además, se observa un perímetro de seguridad física que delimita el ámbito de trabajo y existen controles que sugieren una restricción de acceso.

A partir de las entrevistas realizadas, la observación participante y directa y los controles planteados por la normativa ISO 27001, se presentan los principales hallazgos.

5.2 Controles organizativos

Son de índole general y se enfocan en la manera en la que la organización aborda la seguridad de la información a nivel estratégico y operativo.

De los 37 controles organizativos, se identificaron 22 aplicables al sector. De estos últimos, la mayoría posee una madurez del tipo “gestionado”, lo que implica que se llevan a cabo en base a las buenas prácticas y la experiencia.

No se evidenció que en todos los casos existan procedimientos definidos y documentados que establezcan el accionar de las personas involucradas.

Table 2. Grado de madurez de los controles organizativos

Control	Madurez
5.1 - Políticas de SI	Inexistente
5.2 - Roles y responsabilidades de la SI	Gestionado
5.3 - Segregación de tareas	Gestionado
5.4 - Responsabilidades de la dirección	Gestionado
5.5 - Contacto con autoridades	Gestionado
5.6 - Contacto con grupos de interés especial	Inexistente
5.7 - Inteligencia de amenazas	N/A
5.8 - SI en la gestión de proyectos	N/A
5.9 - Inventario de información y activos asociados	Inicial
5.10 - Uso de la información y activos asociados	Inicial
5.11 - Devolución de activos	N/A
5.12 - Clasificación de la información	Inexistente
5.13 - Etiquetado de información	Inexistente
5.14 - Transferencia de información	Inicial
5.15 - Control de acceso	Gestionado
5.16 - Gestión de identidad	Gestionado
5.17 - Información de autenticación	Gestionado
5.18 - Derechos de acceso	Gestionado
5.19 - SI en las relaciones con los proveedores	N/A
5.20 - Abordar la SI en acuerdos con proveedores	N/A
5.21 - Gestión de la SI en la cadena de suministro de las TIC	N/A
5.22 - Seguimiento, revisión y gestión de cambios de servicio de proveedores	N/A
5.23 - SI para el uso de servicios en la nube	N/A
5.24 - Planificación y preparación para la gestión de incidentes de SI	Inexistente
5.25 - Evaluación y decisión sobre eventos de SI	N/A
5.26 - Respuesta a incidentes de SI	N/A
5.27 - Aprendizaje de los incidentes de SI	N/A
5.28 - Recolección de evidencia	N/A
5.29 - SI durante una disrupción	N/A
5.30 - Preparación de las TIC para la continuidad de negocio	N/A
5.31 - Identificación de requisitos legales, estatutarios y contractuales	Definido
5.32 - Derechos de propiedad intelectual	N/A
5.33 - Protección de registros	Gestionado
5.34 - Privacidad y protección de la información. de identificación personal (PII)	Gestionado
5.35 - Revisión independiente de SI	Definido
5.36 - Cumplimiento de políticas y estándares de SI	Inexistente
5.37 - Procedimientos operativos documentados	Inexistente

Nota: Elaboración propia

5.3 Controles de personas

Tienen como objetivo gestionar y controlar las actividades que realizan las personas que tienen acceso a los sistemas, datos y otros activos de información.

Se pudo observar que de 8 controles, 7 de ellos resultan aplicables. En general se evidencia un bajo nivel de madurez de los mismos, es decir, su aplicación se basa en el esfuerzo personal y las buenas prácticas.

Table 3. Grado de madurez de los controles de personas

Control	Madurez
6.1 - Verificación de antecedentes (screening)	Definido
6.2 - Términos y condiciones de empleo	Inicial
6.3 - Concientización, educación y entrenamiento en SI	Inexistente
6.4 - Proceso disciplinario	Inicial
6.5 - Responsabilidades tras la desvinculación o cambio de empleo	Inexistente
6.6 - Acuerdos de confidencialidad o no divulgación	Inexistente
6.7 - Trabajo remoto	N/A
6.8 - Reporte de eventos de SI	Inicial

Nota: Elaboración propia

5.4 Controles físicos

Tienen como objetivo reducir el riesgo de acceso no autorizado o daño físico a la información. Los equipos e instalaciones de procesamiento de información crítica o sensible deben mantenerse en áreas seguras, con niveles y controles de acceso apropiados, incluyendo protección contra amenazas físicas y ambientales. Este análisis se basó principalmente en la observación participante activa y directa.

Se evidencia que, del total de 14 controles analizados 11 de ellos resultan aplicables. En su mayoría se sitúan en el nivel “gestionado”.

Table 4. Grado de madurez de los controles físicos

Control	Madurez
7.2 - Ingresos físicos	Inicial
7.3 – Aseguramiento de oficinas, salas e instalaciones	Gestionado
7.4 - Monitoreo de seguridad física	Inexistente
7.5 - Protección contra amenazas físicas y ambientales	Inicial
7.6 - Trabajo en áreas seguras	Gestionado
7.7 - Escritorio despejado y pantalla limpia	Inicial
7.8 - Ubicación y protección de equipos	Gestionado
7.9 - Seguridad de los activos fuera de las instalaciones	N/A
7.10 - Medios de almacenamiento	N/A
7.11 - Instalaciones de soporte	Inexistente
7.12 - Seguridad del cableado	Gestionado
7.13 - Mantenimiento de equipos	N/A
7.14 - Eliminación segura o reutilización de equipos	Gestionado

Nota: Elaboración propia

En cuanto al análisis previsto en esta investigación, se hace mención a que teniendo en cuenta el grado de implementación de los controles aplicables y tomando como marco de referencia el CMMI (por sus siglas en inglés “Capability Maturity Model Integration”, integración de los modelos de madurez de capacidades), se arribó a que el nivel de madurez de seguridad de la información del área se encuentra clasificado como “Gestionado” o “Repetible”. El mismo se caracteriza por aplicar buenas prácticas basadas en la experiencia. De este modo, los procesos son impredecibles o “ad hoc”, poco controlados y no están gestionados en todos los casos. Por estos motivos, las actividades o métodos demuestran que no se tienen considerados los requisitos de un marco de cumplimiento o estándar reconocido internacionalmente, como ser ISO 27001 o NIST.

Se considera importante que la Dirección Alumnos pueda realizar una serie de acciones correctivas que le permitan fortalecer su seguridad de la información y acceder al siguiente nivel de madurez denominado “definido”. Esto implica que existan procedimientos establecidos, aprobados, documentados y comunicados a las partes interesadas que regulan las labores habituales de los colaboradores de la organización. Asimismo, debería evidenciarse la existencia de mayores controles y la formación y concientización al respecto.

A tales efectos, se recomienda implementar las acciones detalladas a continuación. Cabe destacar que el criterio tomado para el ordenamiento de las recomendaciones no se fundamenta en su criticidad, sino en el nivel de madurez identificado durante la revisión llevada a cabo y en la secuencia de los controles del Anexo “A” de la norma ISO 27001.

5.5 Acciones críticas

Controles Organizacionales

.

- Políticas de Seguridad de la Información: deben definirse, aprobarse, publicarse y comunicarse a las partes interesadas. Asimismo, deben revisarse en los intervalos planificados o si ocurren cambios significativos.
- Contacto con grupos de interés especial: el sector objeto de estudio debería establecer y mantener contacto con grupos de intereses especiales u otros foros y asociaciones profesionales especializadas en seguridad de la información.
- Clasificación de la información: la información debe clasificarse en términos de confidencialidad, integridad, disponibilidad y otros requisitos exigidos.
- Etiquetado de información: se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado. Se recomienda adaptar el protocolo de semáforo (TLP) de "First".
- Planificación y preparación para la gestión de incidentes de SI: se deben definir, establecer y comunicar procesos de gestión de incidentes de seguridad de la información, incluyendo roles y responsabilidades.
- Cumplimiento de políticas y estándares de SI: se debe revisar periódicamente el cumplimiento de las políticas y estándares de seguridad de la información aplicables al sector objeto de estudio.

Controles de Personas

.

- Concientización, educación y entrenamiento en SI: todo el personal del sector y las partes interesadas deben recibir educación y capacitación adecuadas en materia de seguridad de la información y actualizaciones periódicas de las políticas y procedimientos pertinentes, según sea relevante para su función laboral.
- Responsabilidades tras la desvinculación o cambio de empleo: las responsabilidades y deberes de seguridad de la información que siguen siendo válidos tras la desvinculación o el cambio de empleo deben definirse, hacerse cumplir y comunicarse al personal relevante y otras partes interesadas.
- Acuerdos de confidencialidad o no divulgación: los requisitos para acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados periódicamente y firmados por el personal involucrado y las partes interesadas.

Controles Físicos

.

- Monitoreo de seguridad física: se deben implementar medios para monitorear continuamente la seguridad de las instalaciones.

- Instalaciones de soporte: el equipamiento debe protegerse contra cortes de energía y otras interrupciones causadas por fallas en las instalaciones de soporte.

5.6 Acciones a corto plazo

Controles Organizacionales

.

- Inventario de información y activos asociados: se deben identificar la información y los activos asociados, relevantes para la preservación de la seguridad de la información y sus propietarios. Se debe desarrollar, mantener y utilizar un inventario de estos activos.
- Uso de la información y activos asociados: se deben identificar, documentar e implementar reglas para el uso aceptable y procedimientos para el manejo de información y los activos asociados.
- Transferencia de información: deben existir reglas, procedimientos o acuerdos de transferencia de información, tanto dentro de la organización como entre la organización y otras terceras partes, para todos los tipos de transferencia.

Controles de Personas

.

- Términos y condiciones de empleo: los acuerdos contractuales con el personal deben establecer sus responsabilidades y las de la organización para la seguridad de la información.
- Proceso disciplinario: debe existir un proceso disciplinario formal y comunicado para tomar medidas contra aquellas personas que hayan cometido una violación de la política de seguridad de la información o normativas aplicables.
- Reporte de eventos de SI: la organización debe proporcionar un mecanismo para que el personal de la Dirección Alumnos informe oportunamente los eventos de seguridad de la información observados o sospechados a través de los canales apropiados.

Controles Físicos

.

- Ingresos físicos: el área de trabajo debe permanecer protegida por controles de entrada y puntos de acceso adecuados.
- Protección contra amenazas físicas y ambientales: se debe diseñar e implementar protección física contra eventos indeseables como desastres naturales, ataques físicos, vandalismo o accidentes.
- Escritorio despejado y pantalla limpia: deben definirse y aplicarse reglas de escritorios despejados de papeles y reglas de pantallas limpias para las instalaciones de procesamiento de información.

5.7 Acciones a mediano plazo

Controles Organizacionales

.

- Roles y responsabilidades de la SI: todos los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades del sector y teniendo en cuenta la segregación de las tareas.
- Responsabilidades de la dirección: la dirección del sector debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con las normas y los procedimientos establecidos.
- Gestión de identidad: se debe gestionar el ciclo de vida completo de todas las identidades para el acceso a los sistemas informáticos.
- Información de autenticación: la asignación y gestión de la información de autenticación debe controlarse mediante un proceso de gestión formal, que incluya asesorar al personal sobre el manejo adecuado.
- Derechos de acceso: los derechos de acceso a información, sistemas, aplicaciones y servicios deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con los procedimientos sobre control de acceso.
- Protección de registros: los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legales, reglamentarios, contractuales y comerciales.

Controles Físicos

.

- Asegurar oficinas, salas e instalaciones: deben diseñarse e implementarse procedimientos para trabajar en áreas seguras. El equipamiento debe ser ubicado de forma segura y protegida.
- Seguridad del cableado: el cableado de energía y telecomunicaciones que transporta datos o soporte a servicios de información debe protegerse contra intercepciones, interferencias o daños.
- Eliminación segura o reutilización de equipos: todos los elementos del equipamiento que contienen medios de almacenamiento deben verificarse para garantizar que los datos confidenciales y el software licenciado hayan sido eliminados o sobrescritos de forma segura antes de su descarte o reutilización.

6 Conclusiones

En el presente trabajo se identificaron los controles de seguridad de la información aplicables al sector objeto de estudio, teniendo en cuenta las buenas prácticas propuestas por CIS y el anexo “A” de la norma ISO 27001. A partir de ello, se efectuó un análisis de estos y se estableció un nivel de madurez enfatizando en los controles organizacionales, de personas y físicos (ambientales y documentales).

A partir de las herramientas metodológicas aplicadas y el análisis anteriormente desarrollado, se infiere que el nivel de madurez de seguridad de la información de Dirección Alumnos de la Facultad de Ciencias Económicas (UNT), se enmarcaría en la clasificación de "Gestionado". A partir de ello, se recomienda que el sector implemente una serie de acciones correctivas que le permitan fortalecer su seguridad de la información y acceder al siguiente nivel de madurez denominado "Definido". Esto implicaría que existan procedimientos establecidos, aprobados, documentados y comunicados a las partes interesadas que regulan las labores habituales de los colaboradores de la organización. Asimismo, debería evidenciarse la existencia de los controles detallados anteriormente y la formación y concientización al respecto.

Teniendo en cuenta el contexto actual caracterizado por la complejidad y el aumento de amenazas informáticas, se enfatiza en la importancia de implementar controles de seguridad de la información eficaces. Debido a la criticidad y sensibilidad de los datos que gestiona el área, un incidente podría ocasionar, entre otros, un impacto para la institución y sus partes interesadas, inconvenientes para asegurar la continuidad de sus operaciones o demandas por incumplimientos legales relacionados a la inadecuada protección de los datos.

Por lo tanto, es fundamental implementar medidas de seguridad de la información y mantener un nivel adecuado de madurez, para asegurar la integridad, confidencialidad y disponibilidad de la información.

Se pone de manifiesto la importancia de la identificación y tratamiento del riesgo para una adecuada dirección estratégica de la institución, lo que contribuiría a evitar incidentes que comprometan las características de la información segura y otorgar confianza a los usuarios, demostrando que los peligros identificados se gestionan apropiadamente.

Se espera que los resultados de este trabajo contribuyan al conocimiento de la situación actual y a la implementación de acciones por parte de las autoridades que tiendan al fortalecimiento de seguridad de la información en la institución.

7 Referencias bibliográficas

1. Center for Internet Security. (2021). *Controles de seguridad críticos de CIS (Versión 8)*. https://www.cisecurity.org/controls
2. First (2022). *Traffic Light Protocol (TLP): First Standards Definitions and Usage Guidance – Version Versión 2.0*. https://www.first.org/tlp/
3. Instituto Nacional de Ciberseguridad de España (18 de mayo de 2021). *Glosario de términos de ciberseguridad: una guía de aproximación para el empresario*. https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario
4. Instituto Nacional de Ciberseguridad de España. (s.f.). *Traffic Light Protocol (TLP)*. https://www.incibe.es/incibe-cert/sobre-incibe-cert/tlp#:~:text=Traffic%20Light%20Protocol%20(TLP)%20es,la%20seguridad%20de%20la%20informaci%C3%B3n.
5. Instituto Argentino de Normalización y Certificación (2018). *Norma ISO 31000. Gestión del riesgo. Principios y Directrices*. Autor

6. Instituto Argentino de Normalización y Certificación. (2021). Norma ISO 27002: Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para los controles de la seguridad de la información. Autor.
7. Organización Internacional para la Estandarización y Comisión Electrotécnica Internacional. (2018). *ISO/IEC 27000: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Descripción general y vocabulario*.
8. Organización Internacional para la Estandarización y Comisión Electrotécnica Internacional. (2022). *ISO/IEC 27001. Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos*.
9. Laudon, K. y Laudon J. (2016). *Sistemas de Información Gerencial* (14º ed.). Pearson.
10. Instituto Nacional de Estándares y Tecnología. (2019). Marco de cumplimiento Cobit 2019: introducción y metodología.
11. Instituto Nacional de Estándares y Tecnología. (2019). Marco de referencias en ciberseguridad (5°ed.).
12. Capability Maturity Model Integration. (25 de junio de 2023). En *Wikipedia*. https://es.wikipedia.org/w/index.php?title=Capability_Maturity_Model_Integration&direction=prev&oldid=153931074