Política Seguridad de la Información

Institución Internacional de Altos Estudios León Cooper – IAE COOPER

CONTENIDO

1. PRESENTACIÓN 3
2. MARCO GENERAL 3
2.1. Marco Conceptual 4
2.2. Marco Jurídico 5
2.3. Alcance 5
3. OBJETIVOS 6
3.1. Objetivo general 6
3.2. Objetivos específicos 6
4. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN 6
4.1. Calidad de los datos 8
4.2. Administración de datos. 9
4.2.1 Datos Maestros 9
4.2.2 Datos de Referencia 9
4.3. Seguridad digital para la gestión de talento humano 10
4.4. Gestión de activos de la información. 10
4.5. Control de acceso digital. 11
4.6. Gestión de la seguridad física y del entorno 12
4.7. Gestión de la seguridad de las operaciones. 12
4.8. Seguridad de las Comunicaciones 13
4.9. Gestión de Incidentes de la Seguridad de la Información. 13
4.10. Gestión de disponibilidad tecnológica. 14
4.11. Privacidad y Protección de Datos Personales. 14
4.12. Cumplimiento de requisitos legales y contractuales. 15
4.13. Revisiones de Seguridad de la Información y Protección Datos Personales. 15
4.14. Divulgación, cultura y adopción de Seguridad Digital y Protección de Datos Personales. 16
4.15. Deberes y sanciones. 16
5. RESPONSABLES DE LA POLÍTICA 16
5.1. Responsables de la gestión administrativa de la política 16
6. SEGUIMIENTO Y EVALUACIÓN 17
6.1. Evaluación de la política 18
6.2. PQRSF 18
6.3. Planes de mejoramiento 18

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. PRESENTACIÓN

En la Institución Internacional de Altos Estudios León Cooper – IAE COOPER, la protección de la información se convierte en una prioridad fundamental. Nuestro enfoque se centra en la reducción del impacto causado por riesgos que hemos identificado de manera sistemática. Esto se lleva a cabo con el propósito principal de mantener un nivel mínimo de exposición, lo que nos permite garantizar la integridad, confidencialidad y disponibilidad de la información de manera efectiva y constante.

Comprendiendo la importancia y el compromiso de preservar la Seguridad de la Información, la Ciberseguridad y la Protección de los Datos Personales en el desarrollo de las actividades que apoyan la gestión académica y administrativa de la Institución se considera pertinente actualizar y reglamentar las principales políticas y directrices en relación con aspectos generales de la gestión y administración de la seguridad de la información.

Además de lo mencionado previamente, se presenta una demanda constante de información para satisfacer requerimientos externos de entes como: el Ministerio de Educación Nacional, procesos de acreditación, de calidad, entre otros, e Internos, tales como: la generación de boletines estadísticos, la rendición de cuentas, la planificación de actividades institucionales, el plan de desarrollo institucional, etc., todos estos de suma importancia para el funcionamiento eficaz de la institución.

Como respuesta al contexto previamente expuesto, se formula la Política de Seguridad de la Información. El objetivo es establecer directrices estratégicas que aborden los desafíos institucionales y que promuevan la gobernanza efectiva de los datos y la información. Su enfoque se centra en fortalecer la toma de decisiones, garantizar la rendición de cuentas y satisfacer las necesidades cotidianas para el óptimo funcionamiento de IAE COOPER en esta línea.

Este documento identifica varios actores involucrados en la seguridad de la información y busca establecer un conjunto de prácticas y directrices destinadas a mantener la seguridad informática de IAE COOPER e instituciones con las cuales desarrolle acuerdos.

2. MARCO GENERAL

En consonancia con la filosofía de calidad en IAE COOPER, la cual se entiende como el nivel de coherencia entre la identidad institucional, lo plasmado en el Plan de Desarrollo Institucional 2020-2027 (PDI) y en el Proyecto Educativo Institucional (PEI) y las acciones llevadas a cabo en la cotidianidad, se busca instaurar una cultura que contribuya a la mitigación del riesgo y la disminución del impacto, en las actividades que deben estar protegidas de amenazas, que puedan ocasionar pérdida de información, pérdidas financieras, daños a la

reputación o exposición de información confidencial, adoptando acciones preventivas para los riesgos previamente identificados y garantizar las respectivas revisiones sobre los mismos para adaptarse a los cambios que se produzcan en el entorno, los procesos y las tecnologías de información.

Igualmente, se busca reconocer y gestionar los riesgos que eventualmente puedan surgir, fortaleciendo y apoyando la continuidad de los procesos, alineados a los objetivos institucionales, y a los requerimientos regulatorios acorde a la Ley de Protección de Datos Personales y buenas prácticas como la norma ISO 27001:2013. Entre los objetivos que persigue esta política es el de establecer los lineamientos necesarios para proteger y administrar de manera correcta el uso de la información, así como el manejo adecuado de las tecnologías utilizadas para el procesamiento de la información, asegurando así que los servicios de IAE COOPER, se presten de manera eficiente y no se afecte la continuidad de su operación, cumpliendo con las obligaciones legales y reglamentarias. Así como dar respuesta a los requerimientos, necesidades del entorno y la sociedad en general.

En este contexto, esta política representa una iniciativa preventiva y estratégica, orientada a anticipar y mitigar cualquier eventualidad, suceso o circunstancia que pueda poner en riesgo la integridad, confidencialidad y disponibilidad de la información, así como la salvaguardia de los datos personales.

2.1. Marco Conceptual

Esta política parte del reconocimiento que los datos institucionales son un activo estratégico, es decir, la base fundamental para obtener información relevante sobre la comunidad universitaria, el entorno, las acciones, tendencias y el cumplimiento de los objetivos de IAE COOPER. Los datos se consideran una herramienta clave para impulsar la innovación y lograr los objetivos estratégicos. Este reconocimiento conlleva la necesidad de establecer un sistema de gestión, gobierno y uso de estos datos, garantizando su apropiada ética y responsable utilización, bajo la supervisión de un órgano que asegure la calidad, objetividad, legalidad, preservación y actualización de datos.

Dentro del marco conceptual se tienen en cuenta varias referencias sobre la seguridad informática de las cuales se adoptan algunos estándares o guías para la implementación de esta política, así:

- Norma Técnica 27001:2022, que sustituye 27001:2013. "Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información - Requisitos"

- El SGSI es la sigla de Sistema de Gestión de la Seguridad de la Información, cuyo alcance es el diseño, implementación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad a la información, buscando asegurar la confidencialidad, la integridad y la

disponibilidad de los activos de información, además de minimizar los riesgos de seguridad.

2.2. Marco Jurídico

La Política de Seguridad de la Información, la ciberseguridad y la protección de datos personales responde a los requerimientos y disposiciones normativas nacionales e internacionales, así como, se adoptan algunos estándares o guías como un conjunto de orientaciones así:

Normatividad externa.

a. Ley 30 de 1992, artículo 4, 28 y 29. Fines del saber y autonomía universitaria.

b. Ley 527 de 1999 y Decreto 2364 de 2012 sobre la firma electrónica.

c. Ley 1273 de 2008 Delitos informáticos y protección el bien jurídico o tutelado que es la información

d. Ley 1266 de 2008 Habeas data información financiera y seguridad de datos personales

e. Ley 1581 de 2012 Protección de datos personales y Decreto 1377 de 2013 que reglamenta parcialmente la ley.

f. Decreto 1377 de 2013 que reglamente parcialmente el Régimen General de Protección de Datos Personales.

g. Resolución 15224 de 2020 Ministerio de Educación Nacional. Por la cual se establecen los parámetros de autoevaluación, verificación y evaluación de las condiciones de calidad de carácter institucional reglamentadas en el Decreto 1075 de 2015, modificado por el Decreto 1330 de 2019, para la Marco Institucional

A este respecto y con el fin de dar cumplimiento a las directrices institucionales esta tiene dentro de sus referentes los Estatutos Generales, el Reglamento Estudiantil, las Resoluciones y Acuerdos emitidos por el Consejo Directivo y el Plan de Desarrollo Institucional, la Política de Tecnología, Información y Comunicaciones, y la Política de Seguridad de la Información, entre otras.

2.3. Alcance

Esta política es de aplicación para todos los responsables de la obtención, clasificación, almacenamiento, circulación, uso y disposición final de los datos y la información institucional, incluyendo estudiantes, docentes, investigadores, personal administrativo, egresados, proveedores, contratistas, y visitantes que utilicen sistemas de información, aplicaciones, servicios en la nube, datos y redes

de comunicaciones. Así mismo, la presente política se articula, renueva de acuerdo con las disposiciones que emana el Consejo Directivo.

3. OBJETIVOS

3.1. Objetivo general

Orientar y dar lineamientos de seguridad de la información sobre los activos de IAE COOPER, con el fin de garantizar que los riesgos son identificados, valorados y administrados de una forma estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en el entorno y en las tecnologías de información.

3.2. Objetivos específicos

- Establecer la organización administrativa de gobierno con el fin de facilitar una gestión eficaz y eficiente de los datos institucionales y la información, mediante la asignación clara de roles y responsabilidades.

- Fomentar el desarrollo de habilidades en los integrantes de la comunidad académica, enfocándolos en los principios fundamentales y la cultura establecida por esta política. Esto se logrará mediante la promoción de programas de capacitación, formación y orientación dirigidos a aquellos que trabajan con y que gestionan datos.

- Establecer directrices, procedimientos e instructivos que permitan garantizar la calidad de los datos, impulsando su utilización efectiva y cumpliendo con los requisitos de informes tanto a nivel interno como externo.

- Poner en marcha sistemas de seguridad de la información y fomentar la utilización responsable de los recursos tecnológicos.

- Garantizar el acatamiento de las leyes y regulaciones vigentes en la protección de datos personales, así como la utilización ética de los mismos, con el propósito de prevenir sanciones legales, multas y salvaguardar los derechos de los individuos titulares de dichos datos.

- Resguardar la información de IAE COOPER, considerando su nivel de sensibilidad, criticidad y valor.

- Promover la innovación tecnológica con el fin de garantizar la continuidad de los servicios y la seguridad de la información, evitando cualquier interrupción en los servicios tecnológicos de la información y comunicación.

4. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

IAE COOPER considera los principios de seguridad de la información como elementos esenciales para proteger la privacidad y la integridad de los datos

sensibles de la institución, así como para garantizar su disponibilidad cuando sea necesario. La confidencialidad asegura que la información sensible esté protegida contra accesos no autorizados, como datos financieros y personales de estudiantes, docentes, colaboradores y demás comunidad que tenga acceso a la red y recursos de la institución. La integridad, por otro lado, garantiza que la información sea precisa y esté protegida contra modificaciones no autorizadas, lo que es crucial para mantener la confianza en los datos y respaldar la toma de decisiones informadas.

Además, estos principios ayudan a cumplir con las leyes y regulaciones relacionadas con la privacidad y la protección de datos, evitando sanciones legales y daños a la reputación de la institución. También proporcionan un marco para identificar, evaluar y mitigar las amenazas a la seguridad de la información, incluyendo ciberataques y desastres naturales, y gestionar de manera efectiva los riesgos asociados con el manejo de la información.

Entre los principios tenidos en cuenta por parte de IAE COOPER se encuentran los siguiente:

- **Autorregulación:** Se espera que todos los usuarios actúen de manera responsable y ética en el manejo de los recursos y datos de la institución, siguiendo las políticas y procedimientos establecidos para garantizar la protección de la información.

- **Confidencialidad:** La confidencialidad es un pilar esencial de la política de seguridad de la información. Se garantiza que la información sensible y privada esté protegida contra accesos no autorizados, asegurando la privacidad de las personas y la integridad de los datos institucionales.

- **Integridad:** La integridad de la información es crucial para mantener la confianza en los datos de IAE COOPER. Por lo que se desarrollan procedimiento para proteger la exactitud y la consistencia de la información, asegurando que no sea alterada de manera no autorizada y que permanezca completa y fiable en todo momento.

- **Disponibilidad:** IAE COOPER se compromete a garantizar que la información esté disponible y accesible cuando sea necesaria para llevar a cabo las actividades académicas y administrativas de manera oportuna y eficaz.

- **Responsabilidad:** Todos los usuarios de la información de IAE COOPER tienen la responsabilidad de protegerla y manejarla de manera segura y ética. Se espera que cada individuo comprenda y cumpla con sus responsabilidades en materia de seguridad de la información, contribuyendo así a la protección de los activos de la institución.

- **Cumplimiento Legal:** IAE COOPER es galante del cumplimiento de todas las leyes y regulaciones aplicables en materia de seguridad de la

información. Esto incluye el cumplimiento de normativas como el Decreto 1330 de 2019 y otras disposiciones legales relacionadas con la protección de datos y la privacidad.

- **Protección:** IAE COOPER implementa medidas de seguridad adecuadas para proteger la información contra amenazas internas y externas, incluyendo ciberataques, intrusiones y otros riesgos de seguridad. Además, administrar adecuadamente la información confidencial y privilegiada.

- **Seguridad:** En la gobernanza de datos e información, se debe considerar la integración con las normativas de IAE COOPER en lo que respecta a la Política de Seguridad de la Información.

- **Difusión**: IAE COOPER establecerá junto con la Oficina de comunicación institucional una línea de comunicación y entrenamiento destinado a capacitar a su personal en los principios, procesos, objetivos y estándares relacionados con la gestión de la información.

4.1. Calidad de los datos

IAE COOPER fomenta la utilización de datos oportunos, disponibles, precisos y con, confiables, completos y adecuados para su uso previsto. Ya que estos influyen directamente en la toma de decisiones, la eficacia de los procesos, el reporte ante organismos internos y externos. Para de esta manera proporcionar servicios eficaces y eficientes en las diferentes áreas de IAE COOPER.

De acuerdo con lo anterior IAE COOPER determina algunas dimensiones de la calidad de los datos como son:

- **Completitud**. Los datos necesarios se encuentran íntegros en términos de sus atributos. Por ejemplo, todos los docentes disponen de un número de teléfono de contacto, sin excepciones, sin correos electrónicos faltantes o sin números de teléfono - ausentes.

- **Consistencia.** Los datos mantienen una representación uniforme en todo el conjunto de información. Por ejemplo, en un sistema de información, el centro de costos de un profesor se identifica como "su número de documento", y esta misma información se mantiene consistente al cruzarla con otros sistemas.

- **Exactitud.** Los datos reflejan de manera precisa los valores auténticos de la información. Por ejemplo, los nombres y apellidos coinciden con los registrados en el documento de identidad de la persona.

- **Pertinencia temporal.** Los datos se encuentran disponibles cuando se necesitan. Por ejemplo, en caso de requerir un informe para entidades externas como el MEN, la información puede ser accedida desde algún sistema de manera oportuna.

- **Unicidad.** Los datos se identifican y registran de manera precisa en una única ocasión, por lo tanto, no puede haber datos duplicados o repetidos con el fin de evitar redundancia e inconsistencia.

- **Validez.** Los datos cumplen con la sintaxis establecida en su definición, incluyendo el formato, el tipo y el rango adecuados. Por ejemplo, la fecha de nacimiento es una fecha válida (Error en fecha: 31 de febrero).

4.2. Administración de datos.

IAE COOPER gestiona los datos a partir de los conceptos de datos maestros y datos de referencia teniendo en cuenta las diferentes funciones y características:

4.2.1 Datos Maestros

Es importante indicar que los datos maestros son un conjunto de datos clave que representan la información fundamental y centralizada de la institución. Estos datos son utilizados como fuente única y confiable de información para toda la organización y suelen ser compartidos por múltiples aplicaciones. Los datos maestros suelen incluir información estática y estructurada como estudiantes, docentes, empleados, proveedores, elementos (equipos de cómputo, software, libros), etc. Su objetivo principal es garantizar la consistencia y la integridad de la información en toda la institución, evitando la duplicación y los errores de datos.

Adicional a lo anterior es importante tener en cuenta los siguientes aspectos:

- Son compartidos por los diferentes sistemas de información de la Institución.

- Requieren de limpieza y estandarización mediante los procesos establecidos para garantizar la calidad de estos.

- Deben tener una estrategia para ser desplegados a los diferentes procesos (estratégicos, misionales y de apoyo) que así lo requieran.

4.2.2 Datos de Referencia

Los datos de referencia son conjuntos de datos específicos que se utilizan como puntos de referencia o estándares para categorizar, clasificar o contextualizar otros datos.

Estos datos proporcionan un marco de referencia para IAE COOPER y la interpretación de otros datos y suelen ser utilizados para enriquecer la información y mejorar su calidad. Los datos de referencia pueden incluir listas de códigos, catálogos de productos, tablas de conversión, vocabularios controlados, etc. Su objetivo principal es proporcionar una base común y consistente para la interpretación y el intercambio de datos dentro y fuera de la institución.

Adicional a lo anterior es importante tener en cuenta los siguientes aspectos:

- No necesariamente están centralizados.

- Están integrados con datos maestros.

El Sistema de Información Integral de IAECOOPER - SIIU está compuesto por las siguientes plataformas: Académica – Plataforma de Información Académica, Contable SIIGO, formación virtual IAECOOPER360, Microsoft One Drive y los siguientes repositorios documentales: ELibro de consulta de información de la Institución Internacional, las cuales tendrán el siguiente alcance:

4.3. Seguridad digital para la gestión de talento humano

La seguridad de la información es una responsabilidad compartida en IAE COOPER, y la contribución es fundamental para garantizar que los datos y sistemas estén protegidos de amenazas internas y externas. En este sentido:

- La institución cuenta con procedimientos establecidos para asegurar que los colaboradores y contratistas comprendan y cumplan cabalmente con sus responsabilidades, de acuerdo con los roles y niveles de acceso asignados en los sistemas de información y plataformas tecnológicas. Esta medida es esencial para mantener la seguridad y confidencialidad de los datos y garantizar un entorno de trabajo seguro y productivo.

- Garantiza que los contratos de los colaboradores se incorporen cláusulas que aborden la confidencialidad, la no divulgación de información y el manejo de datos personales. Además, se establece la obligación de cumplir con los controles de seguridad, las políticas y los procedimientos incluso después de finalizar la relación contractual. Esta medida asegura la protección de la información sensible y mantiene un compromiso continuo con la seguridad de datos.

- Asegura que los colaboradores sigan un proceso de desarrollo y adquisición de competencias que les permita comprender plenamente la relevancia de proteger la información y los datos personales de posibles amenazas, tanto en entornos físicos como digitales. Esto promoverá una cultura de seguridad sólida y una mayor conciencia sobre la importancia de salvaguardar los activos de información.

- Desarrolla modelos fundamentados en datos que posibiliten la evaluación del nivel de respuesta en la Comunidad Educativa con el propósito de detectar eventos o incidentes relacionados con la ciberseguridad.

4.4. Gestión de activos de la información.

IAE COOPER propende por una administración efectiva de todos los recursos de información de la institución para garantizar su seguridad, disponibilidad e integridad. Algunos de los ejemplos que hacen parte de estos activos son: bases

de datos de estudiantes o interesados, registros financieros, información de empleados, contratos y documentos legales, por lo tanto, se tiene en cuenta los siguientes aspectos:

- Implementar las prácticas y procesos necesarios para llevar a cabo una gestión integral de los activos de información. Esto abarca desde la identificación, clasificación y registro de los activos según su importancia, la asignación de responsabilidades y propietarios, hasta la custodia y resguardo de dichos activos.

- Clasificar y categorizar los activos de información considerando factores como su valor, nivel de importancia, grado de confidencialidad y los requisitos legales correspondientes.

- Protección y control de activos para establecer controles de seguridad, como firewalls, sistemas de detección de intrusiones, cifrado de datos y políticas de acceso restringido, para proteger los activos de información contra amenazas internas y externas.

4.5. Control de acceso digital.

El control de acceso digital es fundamental en la actualidad para IAE COOPER, ya que garantiza que solo las personas autorizadas puedan acceder a sistemas, datos y recursos digitales. Esto no solo protege la información confidencial de posibles amenazas, sino que también preserva la integridad y la disponibilidad de los activos digitales. Además, contribuye a cumplir con regulaciones de privacidad y seguridad, fortaleciendo la confianza de clientes y socios en la organización, para ello, se propone:

- Garantizar la implementación de procesos y controles que permitan una gestión eficiente del acceso a las plataformas tecnológicas. Esto abarca todo el ciclo de vida de control de acceso de los usuarios, desde su incorporación hasta su desvinculación, siguiendo las directrices establecidas. Estas medidas aseguran la seguridad y la integridad de los sistemas y datos.

- Establecer y mantener al día los perfiles de acceso a la plataforma tecnológica de acuerdo con las necesidades específicas de IAE COOPER. Esta tarea es esencial para garantizar que cada usuario tenga el acceso adecuado y limitado según sus responsabilidades y funciones dentro de la organización.

- Las credenciales de acceso ya sean contraseñas, códigos, tarjetas inteligentes, dispositivos de autenticación, llaves de protección de software o cualquier otro activo de información, son de uso exclusivo y personal. Cada usuario es responsable de su administración, uso y resguardo, ya que no deben ser compartidas ni transferidas a terceros. La

seguridad de estas credenciales es fundamental para proteger los activos de información.

4.6. Gestión de la seguridad física y del entorno

Con respecto de la gestión de la seguridad física y del entorno, es esencial para salvaguardar activos, instalaciones y personal de la institución frente a riesgos y amenazas físicas. En este contexto, se aplican medidas para prevenir incidentes y garantizar la continuidad de las operaciones en un ambiente seguro y protegido, así:

- Implementar medidas de control y restricción de acceso físico adecuadas para prevenir accesos no autorizados y asegurar la protección de las instalaciones, los activos de información y las personas. Esto contribuye a mantener un entorno seguro y resguardado.

- Implementar los procedimientos y controles de acceso físico con el propósito de prevenir cualquier daño, pérdida o robo de los activos de información y tecnológicos pertenecientes a la Institución.

- Poner en marcha medidas que permitan el control adecuado del ingreso y salida de activos de información de las instalaciones de la Institución. Esto garantiza que los activos se gestionen de manera segura y se evite cualquier pérdida o acceso no autorizado a información crítica.

- Establecer y aplicar sistemas de control de acceso en áreas seguras mediante el uso de tecnologías, en conformidad con los procedimientos establecidos por la organización.

4.7. Gestión de la seguridad de las operaciones.

Para IAE COOPER la gestión de la seguridad de las operaciones es un componente vital en el entorno empresarial moderno. Se enfoca en garantizar que las operaciones de una organización se lleven a cabo de manera segura, eficiente y sin interrupciones, al mismo tiempo que se minimicen los riesgos y se protegen los activos y la integridad de la información para que el uso adecuado seguirán las siguientes disposiciones:

- Asegurar la integridad de la plataforma tecnológica mediante el uso de mecanismos de ciberseguridad para prevenir riesgos relacionados con fraude y actividades ilícitas.

- Emplear exclusivamente las herramientas de colaboración y productividad en la ejecución de sus roles y funciones.

- Planificar, implementar y supervisar cambios tecnológicos de forma eficiente, asegurando la continuidad operativa y minimizando posibles interrupciones en los servicios respaldados por la infraestructura tecnológica de la Institución.

- Proteger de manera constante la información institucional contra la pérdida o destrucción de datos, asegurando la realización periódica de copias de seguridad.

- Establecer mecanismos y protocolos que permitan la supervisión y control de los recursos, así como la gestión de capacidades futuras, para garantizar el rendimiento deseado en la infraestructura tecnológica de la Institución.

- Implementar tecnologías emergentes destinadas a fortalecer la protección de sistemas de información, aplicaciones e infraestructura tecnológica contra amenazas cibernéticas y software maliciosos.

- Definir protocolos, pautas, y herramientas o servicios necesarios para identificar vulnerabilidades técnicas en sistemas de información, aplicaciones e infraestructura tecnológica.

- Realizar pruebas de Hacking Ético, ejercicios de intrusión y análisis de vulnerabilidades con el objetivo de detectar posibles brechas de seguridad y elaborar planes de acción para mejorar la seguridad digital en las plataformas tecnológicas.

- Vigilar constantemente la plataforma tecnológica para correlacionar eventos, detectar vulnerabilidades y analizar la ciberseguridad. Esto permite evaluar el estado de los riesgos cibernéticos y desarrollar estrategias para minimizar su impacto en la operación.

4.8. Seguridad de las Comunicaciones

La seguridad en las comunicaciones desempeña un papel importante en el ámbito de la informática y la tecnología de la información en IAE COOPER. Pues en un mundo cada vez más interconectado, donde la transferencia de datos y la comunicación son vitales para el funcionamiento de organizaciones y particulares, es esencial garantizar que la información se transmita de manera segura y confiable, para ello, se propone:

- Definir los estándares, herramientas y procedimientos necesarios para gestionar, supervisar y mejorar de manera eficiente los servicios de conectividad.

- Resguardar la información sensible o confidencial que se transmita tanto dentro como fuera de IAE COOPER mediante la implementación de mecanismos de cifrado.

4.9. Gestión de Incidentes de la Seguridad de la Información.

La gestión de incidentes de seguridad de la información se ha convertido en una preocupación primordial en el entorno, donde la digitalización y la interconexión de sistemas y datos son cada vez más frecuentes. En un mundo donde las

amenazas cibernéticas son una realidad, es esencial contar con un enfoque sólido y efectivo para identificar, responder y mitigar incidentes de seguridad de la información, ante las situaciones que se presenten en IAECOOPER, para ello, se propone:

- Establecer y formalizar el proceso que guiará el análisis, evaluación, documentación de evidencia, tratamiento y notificación de incidentes vinculados a la seguridad de la información, la protección de datos personales y la ciberseguridad, con el propósito fundamental de reducir el riesgo asociado a la vulneración de la confidencialidad, integridad y disponibilidad de la información custodiada por IAE COOPER.

- Igualmente, se hará hincapié en la obligación de notificar cualquier evento o incidente de seguridad de la información, así como de protección de datos y ciberseguridad, que ponga en peligro la continuidad de las operaciones debido a amenazas como el acceso, divulgación, alteración o eliminación no autorizados de información y datos personales, perturbaciones en el funcionamiento habitual de las redes, sistemas de información o recursos informáticos, o la violación de las directrices establecidas en la Política de Seguridad de la Información y demás normatividad vigente.

4.10. Gestión de disponibilidad tecnológica.

Es un aspecto crítico en la gestión de tecnologías de la información y comunicación (TIC), ya que cualquier interrupción puede tener un impacto significativo en la productividad, la satisfacción del cliente y la reputación de IAE COOPER. Esta gestión implica:

- Implementar estrategias de respaldo, recuperación y respuesta ante desastres para minimizar el tiempo de inactividad.

- Propender por la continuidad de los servicios tecnológicos, para ello, se tiene un plan de recuperación ante desastres que garantiza la disponibilidad de las plataformas críticas en caso de interrupción, asegurando así la confiabilidad y eficiencia de las operaciones tecnológicas.

- Mantener los recursos tecnológicos en óptimo estado, implementando controles y herramientas que respalden, monitoreen y planifiquen para futuras necesidades el procesamiento, almacenamiento y concurrencia de datos e información.

4.11. Privacidad y Protección de Datos Personales.

Para IAE COOPER la privacidad y protección de datos se convierten en pilares esenciales para mantener la confianza de la comunidad académica pues permite

preservar la integridad y seguridad de la información sensible, ante esta, se plantea:

- Adoptar la Política de Tratamiento de Datos, ya que IAE COOPER en su firme compromiso con el respeto al derecho de Habeas data de estudiantes, docentes, colaboradores, personas, y aliados adopta esta Política la cual es de aplicación obligatoria en todas las actividades relacionadas con el manejo de datos personales y debe ser rigurosamente acatada por todos los colaboradores, contratistas y terceros vinculados a ella.

- Implementar prácticas de protección de datos y concienciar a la comunidad educativa sobre la importancia de la privacidad en un entorno digital.

Cabe destacar que el incumplimiento de esta política conllevará a amonestaciones.

4.12. Cumplimiento de requisitos legales y contractuales.

El cumplimiento de los requisitos legales y contractuales para IAE COOPER es una prioridad en todas las operaciones y actividades, garantiza la responsabilidad y compromiso, tanto con la ley como con los acuerdos contractuales, para ello:

- Establecer y mantener procesos sólidos y controles efectivos para cumplir con la normativa vigente, tanto a nivel interno como externo.

- Asegurar el acatamiento de los términos establecidos de los acuerdos contractuales. Esto es especialmente relevante en lo que respecta a la seguridad de la información, la ciberseguridad y la protección de datos personales. Áreas en las que se mantiene un compromiso inquebrantable con el cumplimiento normativo y contractual.

4.13. Revisiones de Seguridad de la Información y Protección Datos Personales.

La seguridad y privacidad de los datos son prioridades cruciales en un entorno digital en constante cambio y evolución, por ello, IAE COOPER plantea la necesidad de realizar revisiones que implican evaluaciones periódicas y exhaustivas de los controles de seguridad implementados y las políticas de protección de datos para garantizar que estén actualizados y sean efectivos, para ello, se pretende:

- Efectuar auditorías periódicas de seguimiento en las plataformas tecnológicas, evaluando rigurosamente el cumplimiento de las políticas y la normativa vigente.

4.14. Divulgación, cultura y adopción de Seguridad Digital y Protección de Datos Personales.

Este eje comprende la difusión de información sobre buenas prácticas de seguridad, la creación de una cultura organizacional consciente de los riesgos cibernéticos y la promoción de comportamientos seguros durante la manipulación de datos personales, e información, para ello, se propone:

- Establecer los procedimientos, controles y medios requeridos para asegurar que tanto la comunidad educativa como las partes involucradas estén debidamente informadas y cumplan con la política en cuestión, así como los documentos que la complementan. La transparencia y el entendimiento de estas directrices son esenciales para promover una cultura de cumplimiento en todos los niveles de la organización.

4.15. Deberes y sanciones.

Para IAE COOPER es una prioridad garantizar la responsabilidad y compromiso tanto con la ley como con los acuerdos contractuales, para ello, se pretende:

- Cualquier persona que tenga vínculo con la institución, estará obligado a conocer y cumplir la presente política y demás disposiciones institucionales que la desarrollen y que se encuentren publicados en la página web Institucional.

- Cuando se identifique el incumplimiento de la presente política por parte de un colaborador, se pondrá en conocimiento a la Dirección de Talento Humano para los efectos de su competencia y atribuciones.

5. RESPONSABLES DE LA POLÍTICA

Para asegurar la alineación estratégica y el monitoreo efectivo de la implementación de esta política, es fundamental la colaboración coordinada de diversas áreas de la Institución Internacional de Altos Estudios León Cooper – IAE COOPER.

Asimismo, para la efectiva implementación de esta política, es esencial contar con una colaboración concertada de todas las áreas de IAE COOPER, incluyendo aliados académicos o empresariales con los cuales se pueden tener acuerdos comerciales para lograr un objetivo común para beneficio de ambas partes.

5.1. Responsables de la gestión administrativa de la política

Con el propósito de supervisar y mantener bajo control el rendimiento del Sistema de Gestión de la Seguridad de la Información, teniendo en cuenta elementos de lo estipulado en la norma ISO 27001:2013, se han definido las siguientes funciones, responsabilidades y niveles de autoridad. Estas medidas se implementan para asegurar la seguridad de la información y los datos personales:

Consejo Directivo. Es responsabilidad primordial del Consejo garantizar la seguridad de la información en el ámbito de IAE COOPER. Su función principal radica en salvaguardar la reputación institucional, asegurándose de que se establezcan políticas, lineamientos y procedimientos claros que estén en total conformidad con los requisitos legales y reglamentarios pertinentes para educación.

Rectoría. Desempeña un papel fundamental al gestionar la asignación, aprobación de los recursos requeridos para la adquisición, el mantenimiento y el soporte de la infraestructura informática de la Institución ante el Consejo Directivo.

Secretaria General. En el contexto de la política de seguridad de la información, desempeña un papel clave en la coordinación, implementación y supervisión de aspectos administrativos y legales de la política de seguridad de la información dentro de la organización.

Líder de Tecnología, informática y Comunicaciones. Encargado de establecer, supervisar y dirigir la gestión de innovación en tecnologías de información. Esto se logra a través de la planificación estratégica del área, la generación de proyectos y planes enfocados en la modernización administrativa y la mejora de la infraestructura mediante el aprovechamiento de tecnologías de información, estándares y prácticas óptimas en TIC. Todo esto se realiza con el propósito de respaldar las funciones sustantivas de acuerdo con las últimas tendencias y el Plan de Desarrollo Institucional (PID).

6. SEGUIMIENTO Y EVALUACIÓN

La Institución Internacional de Altos Estudios León Cooper – IAE COOPER adelanta una serie de actividades destinadas al seguimiento y la evaluación estratégica, técnica y financiera. Estas acciones tienen como propósito la mejora continua de los procesos, el estímulo al trabajo colaborativo y la medición precisa de los logros alcanzados en los planes y proyectos institucionales. Por lo anterior, y con relación a la presente Política se formulan las siguientes estrategias de seguimiento y evaluación, así:

- Realizar auditorías internas y, en algunos casos, auditorías externas para evaluar el cumplimiento de las políticas de seguridad informática y comunicaciones propias y de aliados. Identificar posibles brechas o áreas de mejora.
- Analizar los incidentes de seguridad informática y comunicaciones ocurridos para identificar lecciones aprendidas y mejorar las políticas y procedimientos.
- Implementar herramientas de monitoreo para supervisar las actividades de red y detectar cualquier actividad inusual o potencialmente maliciosa.
- Evaluar regularmente el cumplimiento de las políticas y procedimientos de seguridad, y tomar medidas correctivas cuando sea necesario.

El seguimiento constante y la adaptación proactiva de la política de seguridad informática, es esencial, para proteger la infraestructura tecnológica y la información sensible en IAE COOPER ya que el entorno digital está en constante evolución.

6.1. Evaluación de la política

IAECOOPER en pro de la mejora continua de los procesos y como parte de los procesos de autoevaluación aplicara instrumentos de medición a las actividades realizadas, con el fin de determinar la satisfacción de cada uno de los integrantes de la comunidad académica-administrativa. Además, se llevará un registro de asistencia a cada una de las actividades con el fin de poder identificar el nivel de convocatoria, participación e impacto del plan de acción.

6.2. PQRSF

En la página web de la Institución Internacional de Altos Estudios León Cooper – IAE COOPER, contará un botón que permitirá registrar las peticiones, quejas, reclamos, sugerencias y felicitaciones, por parte de los usuarios de los servicios, esto contribuirá para el seguimiento del impacto de las actividades y para generar evolución a las estrategias planteadas en cada uno de los ejes institucionales del Plan de Desarrollo.

6.3. Planes de mejoramiento

IAE COOPER, verificará continuamente los resultados de las diferentes fuentes de información con el fin de determinar la pertinencia de los ejes, estrategias y actividades, a través del cumplimiento de indicadores. Información que es tenida en cuenta para el planteamiento de planes de mejoramiento por parte del consejo académico.

BIBLIOGRAFÍA

Ley 30 de 1992, artículo 4, 28 y 29. Ministerio de Educación Nacional. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://snies.mineducacion.gov.co/1778/articles-391237_Ley_30.pdf

Ley 527 de 1999 y Decreto 2364 de 2012 sobre la firma electrónica. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276#:~:text=%E2%80%9CPor%20medio%20de%20la%20cual,y%20se%20dictan%20otras%20disposiciones.%E2%80%9D

Ley 1266 de 2008 Habeas data. Gestor normativo. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Ley 1581 de 2012 Protección de datos personales. Gestor normativo. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Decreto 1377 de 2013. Gestor normativo. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Resolución 15224 de 2020, Ministerio de Educación Nacional. https://www.mineducacion.gov.co/portal/normativa/Resoluciones/400475:Resolucion-015224-de-24-de-agosto-de-2020

Decreto 1075 de 2015, modificado por el Decreto 1330 de 2019, para la obtención y renovación del registro calificado. Gestor Normativo. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77913

ISO 27001:2013. norma internacional más reconocida para los sistemas de gestión de la seguridad de la información. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://sarlaft.fiduagraria.gov.co/meci_files/ISO%2027001%202013.pdf

Guía de Transición 27001:2022. Carbón Neutral 2023. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.icontec.org/wp-content/uploads/2023/05/UTCER-201587-PLAN-DE-TRANSICION-CLIENTES-v.-2-20230518-2.pdf

Plan de Desarrollo Institucional (PDI) 2020-2027, IAECOOPER

Proyecto Educativo Institucional (PEI) 2023, IAECOOPER

Política de Tecnología, Información y Comunicaciones, 2023. IAECOOPER

Política de Protección de Datos, 2023. IAECOOPER