Política General de Seguridad de la Información

Basado en las Normas ISO 27.001

Actualizada: abril de 2025

Tabla de contenido

Contexto:

El Instituto Profesional Latinoamericano de Comercio Exterior, IPLACEX, es una institución de educación superior chilena, reconocida como tal por el Estado desde 1990, pese a situar las raíces de su proyecto institucional ya en la década de los 80. Desde sus inicios y gracias a la experiencia y fuerte compromiso de sus fundadores, ha logrado desarrollar su proyecto institucional con éxito, alcanzando su plena autonomía en 1998, luego de superar satisfactoriamente las exigencias del proceso de licenciamiento -entonces denominado "acreditación"- desplegando luego un crecimiento sostenido, junto a una amplia cobertura geográfica.

De acuerdo con lo anterior tomando en consideración el plan de desarrollo estratégico institucional, y en particular los objetivos estratégicos, se llega a la conclusión que la información que genera y gestiona IPLACEX constituye un activo estratégico clave para asegurar el desarrollo institucional y la continuidad del negocio. En este contexto, la Política de Seguridad de la Información está orientada a proteger la información institucional en la totalidad de su ciclo de vida (creación, difusión, modificación, almacenamiento, preservación y eliminación), los medios que permiten dicho ciclo y las personas que acceden y/o manipulan la información, con la finalidad de garantizar su integridad, disponibilidad y confidencialidad.

Este documento ha sido elaborado en base a las buenas prácticas recomendadas por la Norma ISO 27.001. Esta política se basa en la norma ISO 27001:2022, integrando los requisitos de gestión de riesgos, seguridad en la cadena de suministro, ciberseguridad y seguridad en la nube.

En este contexto, IPLACEX protegerá los recursos de información y la tecnología usada para su procesamiento, de las amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad del **Registro académico del estudiarte y sus datos personales,** y adicionalmente, poder garantizar la continuidad de los sistemas de información, minimizar riesgos de daño y asegurar el eficiente cumplimiento de sus objetivos estratégicos.

IPLACEX reconoce como activos de información, a todos los elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización, recuperación y destrucción de información de valor para la empresa.

Para su clasificación se consideran los siguientes criterios:

- Nivel de confidencialidad asociada a la información derivados del criterio interno y marco regulador externo.
- Nivel de disponibilidad del recurso en función del número de personas afectadas por indisponibilidad, funcionamiento irregular, pérdida de imagen y tiempo de recuperación.
- Nivel de inversión económica de reposición ante la pérdida.
- Nivel de pérdida de integridad del activo.

Principios de la Política de Seguridad de la Información:

- Promover una cultura institucional orientada a la seguridad de la información.
- Comprometer a la alta dirección en la difusión, consolidación y cumplimiento de la política.
- Establecer los mecanismos para garantizar la Confidencialidad, Integridad y Disponibilidad de la Información relacionada con el **Registro académico del estudiante y sus datos personales**.
- La gestión de la seguridad de la información se basará en la identificación y tratamiento de riesgos, asegurando la implementación de controles adecuados para mitigar amenazas y vulnerabilidades.

Objetivo General:

Asegurar la continuidad de la labor que desarrolla IPLACEX, mediante el resguardo de los activos de información del alcance.

Objetivos Específicos:

Proteger los recursos o activos de información de la institución en todos sus medios de soporte, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información del alcance, como así también:

- ✓ Identificar las vulnerabilidades que amenacen la información que permite la continuidad del negocio y controlarlos al máximo.
- ✓ Determinar y clasificar los activos de información generados por la organización y que permitan mantener la continuidad del negocio, teniendo en cuenta las matrices de riesgos institucionales.
- ✓ Establecer políticas e instructivos que permitan resguardar los activos de información.
- ✓ Definir un Plan de comunicación que permita difundir los alcances y buenas prácticas asociadas a la seguridad de la información institucional.
- ✓ Definir los responsables de los activos de información y los mecanismos de auditoría y control.

Alcance:

La Política General de Seguridad de la Información de IPLACEX, abarca el proceso transversal denominado:

“Registro académico del estudiante y sus datos personales”

que toca los procesos internos denominados.

a) Admisión y Matricula
b) Provisión de Servicio Presencial y a distancia.
c) Certificación y Titulación

Esta política también cubre la seguridad de la información en entornos de computación en la nube y establece requisitos de seguridad para proveedores y terceros que manejen información de la organización.

Responsabilidades:

Todos los directores, jefes, supervisores o colaboradores, sea cual fuere su nivel jerárquico en la institución, son responsables de la aplicación de esta política de seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La política de seguridad de la información es de aplicación obligatoria para todo el personal de la institución que tenga relación con el registro académico del estudiante y sus datos personales, cualquiera sea el área al que pertenezca, y cualquiera sea el nivel de las tareas que desempeñe.

En caso de apreciarse mala fe en la incorrecta utilización de la Información y recursos de su utilización, IPLACEX podrá sancionar al colaborador con medidas que pueden ser desde una amonestación verbal, escrita, anotación en su hoja de vida y hasta la desvinculación de la empresa, además de ejercer las acciones que legalmente le amparen para la protección de sus derechos.

La dirección de TI y la alta dirección garantizarán la implementación de controles de seguridad en la cadena de suministro, así como estrategias de ciberseguridad para prevenir ataques y amenazas digitales.

Revisión y Actualización:

El Comité de Seguridad de la Información, será el encargado de la revisión y actualización de este documento.

Esta Política de Seguridad de la Información, será revisada anualmente o cuando ocurran hechos relevantes que pudiesen cambiar los objetivos de esta Política.

Se realizará una revisión periódica de esta política para asegurar su alineación con los riesgos emergentes, nuevas amenazas cibernéticas y cambios en la infraestructura tecnológica

Gestión del Ciclo de Vida de la Información

Toda la información será gestionada en función de su ciclo de vida, desde su creación hasta su eliminación segura. Se implementarán controles de retención, eliminación y trazabilidad de datos.

Definiciones

a) Activo
Cualquier bien que tiene valor para la organización

b) Disponibilidad
La propiedad de ser accesible y utilizable por una entidad autorizada

c) Confidencialidad
La propiedad por lo que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.

d) Seguridad de la información
La preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como autenticidad, la responsabilidad, la fiabilidad y el no repudio.

e) Evento de seguridad de Información
La ocurrencia detectada en un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

f) Incidente de seguridad de información
Un único evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que tiene una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información.

g) Sistema de Gestión de seguridad de la información
La parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.

h) Integridad
La propiedad de salvaguardar la exactitud y completitud de los activos.

i) Riesgo residual

Riesgo remanente que existe después de que se hayan tomado las medidas de seguridad.

j) Aceptación del riesgo
La decisión de aceptar un riesgo.

k) Análisis de riesgo
Utilización sistémica de la información disponible para identificar peligros y estimar riesgos.

l) Evaluación de riesgo
El proceso general de análisis y estimación de riesgos.

m) Estimación de riesgo
El proceso de comparación del riesgo estimado con los criterios de riesgo, para así determinar la importancia del riesgo.

n) Gestión de riesgo
Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

o) Tratamiento de riesgo
El proceso de selección e implementación de las medidas encaminadas a modificar los riesgos.