Comunicación Oficial 635

agosto 2024

Fecha publicación: 23 de agosto de 2024

IBERO
CIUDAD DE MÉXICO

CONTENIDO

RECTORÍA

RECTORÍA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD IBEROAMERICANA

INTRODUCCIÓN

El crecimiento acelerado de las tecnologías de la información en las organizaciones ha resultado en un ecosistema complejo dentro del cual la información juega un papel importante, proteger la información en sus diferentes formas y a través de diferentes medios (físicos y/o digitales) debe ser una meta organizacional en la que todas y todos participen.

La Seguridad de la información consiste en su protección ante un amplio rango de riesgos a los que se podría encontrar expuesta como parte inherente a su tratamiento, por lo cual, es necesario el establecimiento de directrices y lineamientos que, a la vez que minimicen los riesgos, maximicen las oportunidades institucionales y aporten beneficios directos e indirectos a la Comunidad universitaria y a la sociedad en general.

La Seguridad de la información se caracteriza como la preservación de:

I. Su **confidencialidad**, asegurando que sólo quienes estén autorizados puedan acceder a ésta;

II. Su **integridad**, asegurando que la información y sus métodos de proceso son exactos y completos; y

III. Su **disponibilidad**, asegurando que las personas usuarias tengan acceso a la información y a sus activos asociados cuando lo requieran.

OBJETO

La presente Política tiene como objeto proteger la información de la Universidad Iberoamericana Ciudad de México (en adelante IBERO), en cumplimiento de sus objetivos organizacionales y la regulación aplicable, a través del establecimiento de directrices generales para la preservación de la confidencialidad, integridad y disponibilidad de la información.

De esta Política emanará la normatividad que contendrá las medidas específicas de Seguridad de la información aplicables a la Universidad, mismas que, para su aplicación, sólo podrán mate-

rializarse a través del compromiso y la responsabilidad de las y los integrantes de la Comunidad universitaria.

AMBITO DE APLICACIÓN

La presente Política es aplicable a todo activo de información que la IBERO posea actualmente o en el futuro, y contempla la información tratada por medios físicos y/o electrónicos.

Esta Política, es aplicable para el personal académico, administrativo y de servicio, el estudiantado, las personas prestadoras de servicios y proveedores de la Universidad, así como, a través del instrumento jurídico respectivo, se promoverá su observancia mutua respecto de otras instituciones públicas, privadas o gubernamentales que tengan relación e intercambio de información con la IBERO, en términos de la normatividad universitaria.

RESPONSABILIDADES

A quienes les resulte aplicable la presente política tendrán las siguientes responsabilidades fundamentales, en el ámbito de sus respectivas competencias:

Generales:

I. **Cumplir con la disposiciones universitarias y oficiales** en materia de Seguridad de la información y protección de datos personales, con el fin de evitar su daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado;

II. **Colaborar activamente para preservar** la Confidencialidad, Integridad y Disponibilidad de la información;

III. **Evaluar la pertinencia, necesidad, proporcionalidad y capacidades institucionales**, antes de recibir información de externos para su manejo;

IV. **Identificar y proteger la información** que genere, obtenga, posea, resguarde o administre, así como, evitar su destrucción, divulgación, modificación y utilización no autorizada;

V. **Participar activamente** en las iniciativas, así como en la solución y seguimiento de todo asunto relacionado con la Seguridad de la información;

VI. **Mantener una adecuada organización** de la Seguridad de la información incluyendo sus relaciones con entes externos, así como la gestión documental apropiada o cualquier otro mecanismo de control que contribuya a fortalecer la protección de la información;

VII. **Optimizar el uso y aprovechamiento de los activos** de información, por medio de su identificación, clasificación y valoración, la asignación de responsabilidades sobre su manejo y la adecuada gestión de sus riesgos, por parte de las personas responsables de los mismos;

VIII. **Establecer medidas adecuadas de control de acceso** a los activos de información, de conformidad con lo que se establezca en la normatividad universitaria, tales como documentos físicos o digitales, hardware, redes, equipos, bases de datos y software, entre otros, considerando para ello la gestión de cuentas de usuarios autorizados;

IX. **Mantener mecanismos de protección** que resguarden la seguridad de las instalaciones, ambientes de trabajo, el acceso a las áreas, los controles para el tratamiento de la información y los archivos o documentos físicos;

X. **Mantener en buen estado el** *hardware* que da soporte a las operaciones, procurando de esta forma la seguridad de los activos de información frente amenazas físicas y del entorno;

XI. **Gestionar los riesgos** tecnológicos, de ciberseguridad y operativos, relacionados con los activos que soportan los sistemas de la universidad;

XII. **Colaborar de forma activa** con el personal responsable de identificar, evaluar y gestionar los riesgos relacionados con la seguridad de los activos de información;

XIII. **Implementar estándares y prácticas de seguridad** para nuevos desarrollos, metodologías y procesos formales para la construcción de sistemas, controles criptográficos, gestión de cambios y configuraciones;

XIV. **Establecer un plan y conformar un equipo de respuesta ante incidentes** que puedan afectar la Seguridad de la información, implementando mecanismos de prevención, detección y respuesta, así como los canales de comunicación para la notificación de eventos, vulnerabilidades y amenazas potenciales, para la prevención de las mismas;

XV. **Diseñar y desplegar las estrategias** de recuperación, los análisis de impacto y los planes de contingencia que permitan mantener la continuidad de los objetivos y procesos clave de la Universidad, que son habilitados a través de la infraestructura tecnológica, los procesos, las personas y la información que la conforma; y

XVI. **Mantener un nivel de cumplimiento normativo y técnico suficiente**, que atienda tanto la normatividad oficial como la universitaria vigente, aplicable y asociada a la tecnología, a los sistemas y al manejo de información; considerando el monitoreo y supervisión continua del cumplimiento regulatorio y tecnológico para la adecuada protección de la información que es utilizada, procesada, transmitida y almacenada por la Universidad.

De las Autoridades universitarias:

I. **Fomentar la cultura de Seguridad de la información** al interior de la Universidad, procurando que todo el personal participe y contribuya de forma permanente y proactiva;

II. **Crear, mantener, difundir, concientizar y vigilar la aplicación de esta Política** en todos los niveles jerárquicos establecidos;

III. **Asegurar que existan los recursos** humanos, materiales, financieros y tecnológicos para desarrollar e implementar planes y estrategias en materia de Seguridad de la información;

IV. **Procurar que todo el personal de la IBERO conozca, respete y atienda** la presente Política y las disposiciones específicas que se deriven de la misma, cumpliendo así con el nivel de Seguridad de la información requerido dentro del ámbito de sus responsabilidades;

V. **Procurar que todo el personal posea los conocimientos y experiencia** necesaria para cumplir con las Políticas y medidas de Seguridad de la información establecidas;

VI. **Establecer cláusulas en materia de Seguridad de la información**, acordes a la presente Política, en todos los contratos, convenios y acuerdos que suscriban con proveedores, autoridades oficiales y otros terceros con los que se vincule la IBERO;

VII. **Establecer y mantener la operación de un Comité de Tecnología y Seguridad de la Información**;

VIII. **Gestionar la Seguridad de la información aplicada** al ciclo de vida laboral o de prestación de servicios de las personas a su ingreso, durante su vinculación, al concluir su relación con la Universidad e, incluso, posterior a su término, incorporando los aspectos que se consideren convenientes, a fin de establecer responsabilidades en materia de Seguridad de la información en los contratos y descripciones de puestos; y

IX. **Establecer las sanciones** correspondientes ante el incumplimiento de la presente Política, así como de las medidas de seguridad específicas de conformidad con que los Criterios Institucionales de Delegación de Autoridad en materia de disciplina relativa al orden, los valores personales y comunitarios.

TRANSITORIOS

ÚNICO. La presente Política entrará en vigor a al día siguiente de su publicación en la Comunicación Oficial de la Universidad Iberoamericana Ciudad de México.