ean universidad

Sala General

Acuerdo No. 022
31 de agosto de 2021

Por el cual se expide la nueva Política de Seguridad de la Información de la Universidad Ean.

La Sala General de la Universidad Ean en uso de sus atribuciones estatutarias y considerando:

Que la Universidad Ean mediante el Acuerdo No. 060 de septiembre 17 de 2009, adoptó una Política de Seguridad Informática, en donde se reconoce el valor y la importancia de la información como activo de la organización, para lo cual propone desarrollar acciones que atiendan las buenas prácticas de seguridad y adoptar los controles y medidas necesarias para dar protección a los datos, siempre orientados a generar confiabilidad respetando la privacidad de la información de los diferentes grupos de interés.

Que en 2012, la Universidad Ean a través del Subproceso de Tecnologías de la Información y Comunicación; TIC, formuló como objetivo estratégico la Seguridad de la Información, alineado con el Plan de Desarrollo Institucional. Igualmente, a través de la Resolución Rectoral No. 059 del 5 de Julio de 2012 modifica el Comité de Archivo por el de Comité de Seguridad de la Información y Gestión Documental de la Universidad Ean, en donde se identifica la necesidad de formalizar las directrices y lineamientos para el uso de las Tecnologías de la Información y Comunicación, la promoción y aplicación de las buenas prácticas de seguridad de la información en la institución.

Que en este contexto y amparados por el Reglamento Interno de Trabajo de la Universidad Ean, la Ley Estatutaria 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales y sus decretos reglamentarios, la Ley 23 de 1982 que contiene las disposiciones generales y especiales que regulan la protección del derecho de autor en Colombia, el Decreto Número 884 de 2012 que reglamenta la Ley 1221 de 2008 que promueve y regula el Teletrabajo, la Ley 1273 de 2009 por la cual se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"; la Universidad Ean construye una estructura normativa interna que sirve como herramienta para garantizar el buen uso y la preservación de la infraestructura tecnológica, la información institucional y generación de mecanismos para proteger la información y datos de acuerdo con la normativa vigente, así como, minimizar los riesgos asociados a la ejecución de actividades mediadas por las tecnologías de la información y comunicación.

Que en la sesión de agosto 19 de 2021, el Consejo Superior derogó el Acuerdo No. 060 de septiembre 17 de 2009 mediante el cual adoptó la Política de Seguridad Informática en la Universidad Ean.

Que la Rectoría y la Gerencia General en la sesión de la fecha, presentaron esta política, como un documento interno de la Universidad de obligatorio cumplimiento para todo colaborador, docente, estudiante, graduado, tercero o persona que tenga relación con la Institución, con acceso a los sistemas de información y a sus bases de datos.

Que esta Política de Seguridad de la Información debe ser sometida a permanente revisión y actualización, atendiendo a los nuevos riesgos derivados del uso de nuevas tecnologías y del entorno digital siempre cambiante o siempre que se produzcan cambios en los sistemas de información, el sistema de tratamiento de datos, la organización o el contenido de la información de las bases de datos, que puedan afectar a las medidas de seguridad implementadas. Así mismo, el manual de seguridad de la información que apalanca esta política debe adaptarse en todo momento a la normativa legal en materia de seguridad de la información y de datos personales, adaptándose a los mejores estándares y prácticas vigentes.

Que el incumplimiento de la Política de Seguridad de la Información por parte de colaboradores, estudiantes, docentes, graduados y terceros tendrá consecuencias de acuerdo con el tipo de incumplimiento y estará sujeto a la legislación nacional, la normativa local y la normativa interna aplicable según lo indique la Universidad Ean.

Que es responsabilidad de la Sala General de acuerdo con el literal a. del artículo 20. de los Estatutos de la Institución, fijar la política general de la Universidad Ean.

Que por lo expuesto,

ACUERDA:

ARTÍCULO 1. ° Expedir la nueva Política de Seguridad de la Información de la Universidad Ean

ARTÍCULO 2. ° El presente Acuerdo rige a partir de la fecha de su expedición y deroga las normas que le sean contrarias.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Expedido en Bogotá D.C., el 31 de agosto de 2021.

Herbert Perico Crissien
Presidente

Ana Lucía Gutiérrez López
Secretario

CONTENIDO

1. TERMINOS Y DEFINICIONES[1]

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema u organización.

Ciberseguridad: Es la protección de la infraestructura tecnológica, realizando tratamiento de las amenazas que ponen en riesgo la información que se procesa, se almacena o se transporta por medios digitales y sistemas que se encuentran interconectados.

Cifrado: Proceso de codificación de información sensible para evitar que esta llegue a personas no autorizadas.

Confidencialidad: Propiedad de que la información no está disponible ni sea revelada a personas, entidades o procesos no autorizados.

Control: Políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo aceptable.

Disponibilidad: Principio referente a garantizar que los sistemas de información y los datos estén listos para su uso cuando se necesiten. Capacidad de permanecer accesible en el sitio, en el momento y en la forma en que los usuarios que estén autorizados lo requieran.

Evento: Presencia identificada de una condición de un sistema que indica que la seguridad o los servicios de red y de infraestructura pudieron ser comprometidos o vulnerados, los controles implementados han fallado y/o que no se ha seguido la política de seguridad de la información de la universidad. Por lo general cuando se identifica un evento se determina que aún no se ha materializado un riesgo.

Incidente: Evento o conjunto de eventos de seguridad de la información no deseados o inesperados, que tienen la posibilidad de comprometer la seguridad, debilitar y afectar la capacidad de la universidad para alcanzar sus objetivos. En un incidente si se determina que se ha materializado un riesgo.

Incidente de seguridad en datos personales: Es la vulneración a la infraestructura de información física o tecnológica de un responsable o encargado del tratamiento, que compromete la disponibilidad, integridad o confidencialidad de la información personal contenida en ella.[2]

Integridad: Garantiza que la información no haya sido alterada o modificada por terceros o quienes no estén autorizados para conservar su validez. Mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

ISO 27001: es una norma emitida por la Organización Internacional de Normalización (ISO) que describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

Manual de Seguridad de la Información: documento compuesto por los lineamientos de seguridad de la información que permiten ampliar el conocimiento en temas específicos, comprender mejor el funcionamiento de algo, o tener en cuenta cuales son las mejores prácticas para ejecutar acciones de seguridad de la información.

Política de seguridad de la información: es un documento de alto nivel que denota el compromiso de la alta dirección con la seguridad de la información. Contiene la definición de la seguridad de la información desde el punto de vista de cierta entidad.

Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Es el efecto de incertidumbre sobre los objetivos de una organización y suele considerarse como una combinación de la probabilidad de un evento y su impacto.

Seguridad de la Información: protección que se brinda a los activos de información mediante medidas preventivas con el fin de asegurar la continuidad del negocio y evitar la materialización de los riesgos. Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de la universidad y de los servicios que presta.

SGSI: Sistema de Gestión de la Seguridad de la Información.

Vulnerabilidad: debilidad de un activo o sistema que puede ser explotada por una o más amenazas para causar algún daño.

2. RESPONSABILIDADES

La Política de Seguridad de la Información es aprobada por la Sala General de la Universidad Ean, cualquier cambio, corrección o actualización, deberá ser propuesto en el Comité de Seguridad de la Información y Gestión Documental objeto de revisión del Coordinador de Seguridad de la Información, o quien haga sus veces, posterior algún cambio o actualización será comunicada a toda la comunidad Eanista incluyendo graduados y terceros a través de los diferentes medios que la universidad posee.

El Comité de Seguridad de la Información y Gestión Documental o el que haga sus veces en la Universidad Ean, deberá establecer unas directrices claras para la gestión de la seguridad de la información, a través de la puesta en vigencia y mantenimiento de las políticas de seguridad de toda la organización. Este comité deberá ser un grupo multidisciplinario donde participen representantes de diferentes áreas de la Universidad.

Es responsabilidad del Oficial de Protección de Datos Personales en el marco del Comité de Seguridad de la Información y Gestión Documental, identificar, actualizar y documentar todos los requisitos regulatorios y legales, identificar los controles para cumplir estos requisitos e identificar los riesgos asociados al Tratamiento de Datos Personales.

Se deben identificar las leyes y regulaciones cuando se adquieran e implementen controles criptográficos, licencias, herramientas de auditoría, grabaciones de conversaciones y otros que sean regulados.

Los datos privados de los estudiantes, docentes, graduados, colaboradores y terceros deben ser protegidos de acuerdo con la legislación de nuestro país y conforme a la Política de Tratamiento de Datos Personales de la Universidad.

En caso de ser necesario aplicar una modificación o cambio a las políticas Generales, se requiere de la revisión del Comité de Seguridad de la Información y Gestión Documental y la aprobación de la Sala General de la Universidad Ean, para su implantación y posterior cumplimiento.

De igual forma, se designó un responsable de Seguridad de la información en la Universidad, cuya posición es denominada Coordinador de Seguridad de la Información en cabeza de la Dirección de Tecnologías de la Información y las Telecomunicaciones y la Dirección Administrativa y Financiera de la Universidad, esta persona asegura el mantenimiento permanente de los niveles de seguridad requeridos por la Universidad Ean, además de la seguridad de los distintos sistemas informáticos y de las redes de telecomunicaciones soportadas. En consecuencia, tendrá el compromiso de prevenir, reducir y eliminar la ocurrencia de eventos e incidentes de seguridad de la información y ciberseguridad por acciones inapropiadas o comportamientos ilegales de los distintos usuarios que utilizan o acceden a los recursos de la Universidad.

El Coordinador de Seguridad de la Información es parte del Comité de Seguridad de la Información y Gestión Documental, tiene como responsabilidad primaria documentar, actualizar e implantar las políticas de seguridad. Así mismo, realiza evaluaciones periódicas acerca de la efectividad de estas y propone modificaciones, que sean necesarias para asegurar la protección de información y los activos que se relacionan con ellas en la Universidad Ean.

Estas responsabilidades no sólo competen a la disposición de los distintos intereses que persigue la Universidad, sino también se encuentran en consonancia con las obligaciones legales y éticas que conciernen al buen funcionamiento y privacidad de la información de la Universidad Ean.

3. GENERALIDADES

3.1. Política de seguridad de la información

El propósito de la Política de Seguridad de la Información de la Universidad Ean es sentar las bases para continuar protegiendo sus activos de información de todas las amenazas internas o externas bien sean deliberadas, accidentales o naturales. Esta política busca asegurar los siguientes principios:

3.1.1. Confidencialidad de la información, de manera que únicamente usuarios autorizados tengan acceso.
3.1.2. Integridad de la información, la cual será mantenida, evitando su alteración no autorizada.
3.1.3. Disponibilidad de la información que es asegurada de acuerdo con los requerimientos de los procesos de negocio.
3.1.4. Cumplimiento de las leyes y regulaciones.
3.1.5. Compromiso con el cumplimiento de los requisitos aplicables relacionados con la seguridad de la información.
3.1.6. Cumplimiento de las obligaciones contractuales con nuestros colaboradores, miembros de la comunidad Eanista y demás grupos de interés (clientes, proveedores, etc.).
3.1.7. Entrenamiento, generación de cultura y conciencia a todos los estudiantes, docentes, colaboradores, graduados, contratistas, clientes y proveedores en seguridad de la información y demás grupos de interés.

3.2. Objetivos de seguridad de la información

3.2.1. Preservar la confidencialidad, integridad y disponibilidad de la información en la Universidad Ean.
3.2.2. Determinar y gestionar los riesgos, a través de la adopción de controles y la supervisión efectiva, y las oportunidades que puedan afectar la seguridad de la información e impactar a la Universidad Ean.
3.2.3. Incentivar una cultura de seguridad de la información a la comunidad Eanista y que esta permita generar un valor agregado en todos los procesos de la Universidad Ean.
3.2.4. Ser competitivos y un referente en la educación por medio de plataformas digitales seguras que generen confianza a nuestros estudiantes y clientes.

3.3. Gestión de riesgos de seguridad de la información

La Universidad Ean genera cultura para la gestión del riesgo en seguridad de la información mediante el establecimiento, formalización e implementación de una metodología para la valoración y tratamiento del riesgo.

Todos los activos de información dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) deben ser evaluados al menos una vez al año y/o cuando hay cambios significativos en la Universidad, en especial por los líderes de proceso para determinar en conjunto con la Coordinación de Seguridad de la Información o quien haga sus veces, los controles mínimos requeridos para reducir y mantener el riesgo a un nivel aceptable.

La ejecución, desarrollo e implementación de los controles requeridos para minimizar los riesgos será responsabilidad de los líderes de proceso (propietario), con el apoyo de las diferentes áreas competentes de la Universidad.

La evaluación de riesgos se realizará según se define en la metodología de gestión de riesgos establecida en la Uuniversidad y que se encuentra publicada en el sistema de información de gestión de calidad iSolución o el que esté vigente. Es importante aclarar que siempre se debe estar gestionando los riesgos que se hayan identificado.

3.4. Comité de Seguridad de la información o el que haga sus veces

El Comité de Seguridad de la Información y Gestión Documental fue creado por la Rectoría y actualmente opera bajo los términos y condiciones de la Resolución Rectoral No 051 de 2020. Este comité es presidido por el Director de Tecnologías de la Información y las Comunicaciones y el Coordinador de Seguridad de la Información quienes en conjunto garantizan, implementan y mantienen las políticas, procedimientos y estándares de seguridad de la Universidad para que cumplan con los requerimientos de sus partes interesadas.

3.5. Seguridad relacionada con el recurso humano

Toda la comunidad Eanista incluyendo graduados y terceros que tengan acceso o haga uso de los recursos de la Universidad debe cumplir con las políticas, procedimientos y directrices de seguridad de información de la Universidad Ean, los cuales están publicados en la página web de la Institución o en el sistema de información de gestión de calidad iSolución o el que esté en operación. Cualquier incidente de seguridad de la información ocasionado por el no cumplimiento de estas, tendrá como consecuencia una acción disciplinaria de acuerdo con lo estipulado en el reglamento estudiantil, reglamento docente o reglamento interno de trabajo según el rol del implicado. El área responsable debe:

3.5.1. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran en función de la seguridad de la información.

3.5.2. Verificar los antecedentes de todos los candidatos a un empleo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.

3.5.3. Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.

3.5.4. Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

3.5.5. La alta dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la Universidad.

3.5.6. Todos los usuarios de activos de información de la Universidad deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

3.5.7. Proteger los intereses de la universidad como parte del proceso de cambio o terminación del empleo.

3.5.8. Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.

La Universidad Ean debe capacitar y desarrollar campañas de concientización en seguridad de la información a los estudiantes, docentes, colaboradores, graduados y terceros de acuerdo con las responsabilidades de su función. Es responsabilidad del Coordinador de Seguridad de la información o quién haga sus veces entregar al área de Transformación Organizacional el contenido de la capacitación para que se incluya dicha formación como parte del proceso de inducción además de publicar la política en lugares visibles.

3.6. Uso aceptable de los activos

La Universidad Ean deberá establecer procedimientos de calidad para el acceso y uso aceptable de los activos de información, bajo la gestión de la Coordinación de Seguridad de la Información o quién haga sus veces, con el objetivo de que sean cumplidas por los usuarios tales como:

3.6.1. Identificación de los activos organizacionales y definición de responsabilidades de protección apropiada

3.6.2. Autenticación para su uso

3.6.3. Lista de recursos a los que los usuarios tienen acceso

3.6.4. Dispositivos etiquetados con información del propietario

3.6.5. Lista de productos aprobados por la universidad

3.6.6. Ubicación de las tecnologías en la red

3.6.7. Desconexión automática de sesiones de tecnologías de acceso remoto

3.6.8. Acceso remoto a proveedores sólo cuando este acceso es estrictamente requerido

3.6.9. Desarrollo e implementación de procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la universidad

3.6.10. Prevención de divulgación, modificación, retiro o destrucción de información.

3.7. Clasificación y control de activos

Toda información, almacenada, creada o transmitida con los recursos de la Universidad Ean es de uso exclusivo de la Universidad y debe ser utilizada para el propósito que la institución defina. La Universidad Ean, a través del subproceso de la Coordinación de la Gestión de Proveedores, Infraestructura y Planta Física o quién a haga sus veces; debe mantener un inventario actualizado de los activos de información existentes, con su correspondiente clasificación y propietario en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. Los propietarios de la información son los responsables de la implantación de dicha clasificación. El titular de los datos es reconocido por la universidad quien garantiza de forma eficaz sus derechos.

3.8. Control de acceso a la información y los sistemas

Los controles para el acceso a la información de la Universidad Ean deben ser definidos de acuerdo con su clasificación, mediante usuario y contraseña. Los estudiantes, docentes, colaboradores y terceros deben acceder únicamente a la información que es necesaria para el desarrollo de sus funciones o responsabilidades con base al principio de mínimo privilegio.

La Universidad Ean cuenta con un procedimiento de administración de usuarios para asignar o cancelar los derechos de acceso para todos los sistemas y servicios. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.

Los derechos de acceso a la información, los sistemas y las instalaciones de todos los empleados y terceros se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.

El acceso a la información por parte de terceros debe concederse solamente para las funciones requeridas y con los mecanismos que aseguren, tanto la identidad de quienes realizan el acceso como la confidencialidad, integridad y disponibilidad de la información.

3.9. Seguridad física y del entorno

Toda área o equipo informático donde se procesa información de la Universidad Ean debe cumplir con las directrices funcionales y procedimientos de seguridad física y del entorno establecidos por la Universidad directamente o a través de la compañía de vigilancia que tenga contratada, con el fin de evitar el acceso por personas no autorizadas, daño e interferencia a los recursos e infraestructura de información.

Los colaboradores que trabajan en las modalidades teletrabajo, trabajo en casa o cualquier esquema en el cual se desarrollen actividades por fuera de las instalaciones de la Universidad Ean, realizarán todas las actividades tendientes a garantizar que personas no autorizadas accedan a los equipos o la información contenida en ellos.

3.10. Recursos e infraestructura física para el procesamiento de información

En cualquier recurso o infraestructura física donde se realice procesamiento de la información de la Universidad Ean, se deben cumplir todas las políticas, procedimientos y directrices de seguridad de la información, que garanticen la confidencialidad, integridad, y disponibilidad de la información.

El administrador de cada plataforma es responsable de mantener e implementar los procedimientos y estándares en el ambiente correspondiente, con el apoyo de la dirección de tecnologías de la información y las comunicaciones.

3.11. Seguridad de las operaciones y las comunicaciones

La Universidad Ean en cabeza del Director de Tecnologías de la Información y las Comunicaciones o quién a haga sus veces debe asegurar el correcto funcionamiento de la infraestructura tecnológica que realiza el procesamiento de información, garantizar operaciones correctas y seguras, se debe hacer seguimiento al uso de recursos tecnológicos, realizar los ajustes y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.

Separar los ambientes de desarrollo, pruebas y producción, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional.

Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

Hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.

Elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepcionales, fallas y eventos de seguridad de la información.

Las actividades del administrador y del operador del sistema se deben registrar y los registros se deben proteger y revisar con regularidad.

Implementar procedimientos para controlar la instalación de software en sistemas operativos.

Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la universidad a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

Establecer e implementar el reglamento de instalación de software por parte de los usuarios.

Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.

Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red ya sea que los servicios se presten internamente o se contraten externamente.

Mantener la seguridad de la información transferida dentro de la Universidad y con cualquier entidad externa.

Los acuerdos de confidencialidad o de no divulgación. Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la Universidad para la protección de la información.

3.12. Adquisición, desarrollo y mantenimiento de sistemas de información

Desde la etapa de diseño de los sistemas de información se deben definir los controles requeridos según los requerimientos para el cumplimiento de los estándares técnicos y de seguridad de la información definidos por la Universidad Ean.

La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para prevenir la transmisión incompleta, el enrutamiento errado, la alteración, divulgación, duplicación o reproducción no autorizada de mensajes. Asegurando que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

3.13. Gestión de incidentes de seguridad de la información

Se ha implementado un procedimiento de gestión de incidentes de seguridad de la información para comunicar, dar respuesta, monitorear y establecer la causa raíz de los incidentes; dicho procedimiento está publicado en el sistema de información de gestión de calidad iSolución o el que esté vigente, dicho procedimiento está compuesto por:

3.13.1. Roles y responsabilidades.
3.13.2. Estrategias de comunicación y canales apropiados.
3.13.3. Procedimiento de respuesta a incidentes.
3.13.4. Requerimientos legales y notificación a las Autoridades.
3.13.5. Procedimiento de recuperación.
3.13.6. Procesos de respaldo de información (backup)
3.13.7. Recolección y análisis de evidencia.

El procedimiento de gestión de incidentes de seguridad de la información se revisa por lo menos una vez al año y se realizan las mejoras pertinentes de acuerdo con las lecciones aprendidas tanto de los incidentes simulados como de los reales. Todos los estudiantes, docentes y colaboradores son responsables de observar y reportar los eventos, incidentes, debilidades y el uso inadecuado de los activos de información de la Universidad Ean de acuerdo con el procedimiento establecido.

3.14. Incidentes de seguridad que involucren datos personales

Deben ser reportados por parte de la Oficial de Datos Personales o quien haga sus veces a la Superintendencia de Industria y Comercio dentro de los 15 días hábiles siguientes a su conocimiento. Requiere la adopción de todas las medidas que evidencien la diligencia de la Universidad para evitar o mitigar el daño que pueda causar a la privacidad de los Titulares en los términos de la Ley, la Política de Tratamiento de Datos, el Manual de Directrices y Lineamientos en Datos Personales y del Manual de Seguridad de la Información de la Universidad Ean vigente. La Oficial de Datos Personales o quien haga sus veces, debe llevar una bitácora exacta y soportada de su gestión.

Cuando se observen afectaciones sustanciales a los Titulares debe considerarse la comunicación de estas y la adopción de medidas de seguimiento y monitoreo para evitar efectos que puedan afectar a los Titulares de los datos.

3.15. Continuidad de negocio

La Universidad Ean, debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres. Además, establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación.

Debido a que cualquier interrupción en los procesos de la universidad puede afectar su operación, es responsabilidad de sus directivas aprobar estrategias, soluciones y planes de continuidad de negocio que cubran las actividades esenciales y críticas de la Universidad Ean.

Se deben incluir controles para identificar y reducir riesgos, limitar las consecuencias de los diferentes incidentes y por último asegurar la recuperación inmediata de las operaciones esenciales.

Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

Como parte fundamental del soporte a la Universidad, todos los sistemas de información deben poseer estrategias, soluciones y planes de contingencia con los recursos necesarios que aseguren la continuidad de los procesos académicos, así como el conocimiento de los Planes de Continuidad de Negocio (BCP) de los proveedores que prestan servicios críticos a la Universidad.

3.16. Violaciones a las Políticas de Seguridad de la Información

Cualquier situación que evidencie la violación a las políticas de seguridad de la información por parte de los estudiantes, docentes, colaboradores, graduados o terceros que tengan relación directa o indirecta en el manejo de la infraestructura tecnológica y sistemas de información de la Universidad Ean podrá resultar en un proceso que deberá ser iniciado por parte del líder de proceso, jefe inmediato o responsable del tercero, con base a las evidencias recopiladas las cuales pueden incluir, más no estar limitadas a:

3.16.1. Acción de tipo disciplinario por parte del área que la Universidad ha dispuesto para el efecto según los lineamientos establecidos por el código sustantivo del trabajo, el reglamento estudiantil, reglamento docente o reglamento interno de trabajo según el rol del implicado, las cláusulas especiales que se establezcan con los colaboradores en sus contratos laborales y/o todo aquello que según las leyes colombianas definan como acciones disciplinarias patronales.
3.16.2. Suspensión o acceso restringido a las áreas de procesamiento de la información.
3.16.3. Terminación del contrato de trabajo o relación comercial (Basados en las disposiciones emitidas por las leyes colombianas en materia laboral y el reglamento interno de trabajo).
3.16.4. Demanda de tipo civil o penal como resultado de las acciones de tipo disciplinario.
3.16.5. Asunción de consecuencias legales derivadas de la investigación que adelante la Autoridad.

4. REVISIÓN Y APROBACIÓN DE LA POLÍTICA

Está política será revisada por el Coordinador de Seguridad de la información o quien haga sus veces mínimo cada doce (12) meses; con el fin de asegurar su vigencia y cumplimiento deberá actualizarse en el mismo periodo previo concepto del Comité de Seguridad de la Información y Gestión Documental de la Universidad Ean y aprobación de la Sala General. También se encuentra dispuesta a modificaciones ante cambios en la estructura organizacional para la administración de la seguridad de la información, siempre y cuando cuente con la revisión del Comité de Seguridad de la Información y Gestión Documental de la Universidad Ean y aprobación de la Sala General.