BILINGUAL INTERNATIONAL SUSTAINABLE

SEGURIDAD DE LA INFORMACIÓN

Política para la Seguridad de la Información de la Universidad Politécnica Metropolitana de Puebla

TERMINOS Y CONDICIONES DE USO

Versión original del documento: 1.0.0 (enero 2019)
Versión actualizada del documento: 1.1.0 (marzo 2020)
Versión actualizada del documento: 1.1.1 (Julio 2021)
Versión actualizada del documento 2.0 2023
Versión actualizada del documento 2.1 (marzo 2024)
Versión actualizada del documento 3 (marzo 2025)
Versión actualizada del documento 4 (marzo 2026)

EL DEBIDO CONTROL Y AUTORIZACIÓN DE LA OFICINA DE SISTEMAS.

Introducción

En la actualidad la información de la institución se ha reconocido como un activo valioso y a medida que los sistemas de información apoyan cada vez más los procesos de misión crítica se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos. Nuestra institución, los sistemas y red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude por computadora, espionaje, sabotaje, vandalismo, fuego, robo e inundación. Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes.

La Política de Seguridad de la Información identifica responsabilidades y establece principios y directrices para una protección integral, apropiada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de las Comunicaciones (TIC).

Con esta Política de Seguridad, la Universidad Politécnica Metropolitana de Puebla (UPMP) asume los principios, requisitos y medidas definidos en los ordenamientos jurídicos en que se sustentan las políticas del presente documento, en el entendido que es una referencia efectuada de manera enunciativa más no limitativa:

- Ley Federal de Protección de Datos Personales en Posesión de Particulares y su Reglamento.
- Ley Federal de Transparencia y Acceso a la Información Pública
- Ley de Instituciones de Crédito
- Disposiciones de Carácter General Aplicables a las Instituciones de Crédito.
- Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Nacional Digital, en Materia de Tecnologías de la Información y Comunicaciones, y en la Seguridad de la Información, así como establecer el Manual Administrativo de Aplicación General en dichas materias.
- Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.
- Manual General de Organización de la UPMP.
- Manual Administrativo de Aplicación General en Materia de Control Interno.
- Objetivos y Lineamientos del Sistema Control Interno.
- Código de Conducta.

Con la promulgación de la presente Política de Seguridad de la Información la Universidad Politécnica Metropolitana de Puebla formaliza su compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales.

1. Acerca de la Seguridad de la Información.

La presente Política de Seguridad de la Información, tiene por objeto establecer el marco operativo para la seguridad de la información en la Universidad Politénica Metropilitana de Puebla, en cumplimiento a las disposiciones legales en la materia.

Estas políticas serán de observancia general para todos los involucrados en el manejo de activos de información, entendidos como todos aquellos elementos de información que tienen valor para la institución o que son necesarios para mantener la continuidad de las operaciones de la Universidad Politénica Metropilitana de Puebla, tanto por integrantes de la comunidad universitaria que en el ejercicio de sus funciones den tratamiento a los activos de información , como para aquellos que hagan uso de recursos de Tecnologías de Información y Comunicaciones (TIC).

Los documentos que deriven de este instrumento regulatorio tales como manuales, procedimientos, políticas técnicas, guías, instructivos tendrán el mismo carácter de ser de observancia general.

La UPMP requiere garantizar que los recursos de TIC se encuentren disponibles para cumplir con los propósitos para los que fueron creados, es decir, que no sean modificados o alterados por circunstancias internas o externas, para lo cual se establece la presente política.

La UPMP, en apego a la legislación universitaria y normatividad en la materia, establece acciones para proteger los activos de información frente a riesgos y amenazas conforme a la metodología de evaluación y tratamiento de riesgos, con el fin de mantener la confidencialidad, integridad y disponibilidad de la información contribuyendo a la continuidad de los procesos institucionales.

Con el objeto de asegurar la confidencialidad, integridad, disponibilidad y el uso eficiente de cualquier activo de información, se establece lo siguiente:

- El uso de cualquier activo de información, se ajustará a lo dispuesto en la legislación en la materia referida a la protección de datos personales, propiedad intellectual y, en su caso a las normas establecidas en la Universidad que resulten aplicables;
- La Universidad reconoce el derecho del usuario a la privacidad y la seguridad; por lo que establece las políticas generales de seguridad de información, lo que representa la visión institucional en cuanto a la protección de sus activos de información; y
- Si surgiera la necesidad de intervenir la privacidad de alguna persona durante el curso de alguna investigación de carácter judicial o por el uso inapropiado de los activos de información o de TIC, la Universidad deberá cumplir los procedimientos legales vigentes para hacerlo.
- Quedan fuera del ámbito de aplicación de la presente Política, aquellos dispositivos tecnológicos personales tales como computadoras portátiles, dispositivos móviles, tabletas, celulares, entre otros, sin embargo, estos entrarán en el marco de aplicabilidad, cuando hagan uso de la red institucional.

Para los efectos de la presente política se entiende por:

Confidencialidad: Propiedad o característica consistente en que la información es accesible únicamente para quienes están autorizados, personas, entidades o procesos.

Disponibilidad: Propiedad o característica consistente en que la información se encuentra accesible y disponible cuando lo requiera una entidad autorizada.

Integridad: Propiedad o característica consistente en el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Medidas de seguridad: Conjunto de disposiciones encaminadas a proteger la información de los riesgos, con el fin de cumplir sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

Red institucional: Medios de comunicación que se utilicen dentro y hacia la Universidad para el tratamiento de información entre los sistemas, equipos que la procesan y almacenan.
TIC: Conjunto de tecnologías aplicadas para proveer a las personas de la información y comunicación a través de medios tecnológicos.
Recursos de TIC: Se refiere a los sistemas de información, la infraestructura de telecomunicaciones, la infraestructura de energía eléctrica, equipo de cómputo, climas, sistemas de almacenamiento y dispositivos periféricos.
Usuario: Se considera a toda aquella persona que hace uso de manera directa o indirecta de la información y de los recursos de TIC de la Universidad.

2. Organización para la Seguridad de la Información.

La Universidad Politénica Metropolitana de Puebla garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral la presente política, por medio de la creación de una comisión técnica denominada ***Comité de Seguridad de la Información*** cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:

- **Rectoría.**
- **Secretario Académico.**
- **Secretario Administrativo.**
- **Subdirección de Planeación o Evaluación.**
- **Jefe de Departamento de Servicios Informáticos.**
- **Jefe de Oficina de Soporte Técnico**

En todo caso, dicha comisión o la mesa de trabajo, deberá revisar y actualizar anualmente esta política presentando las propuestas a los directivos de la institución antes mencionados para su aprobación mediante resolución o acto jurídico correspondiente.
Los jefes de cada área, previa identificación y valoración de sus activos de información, son parte responsables de su propia Seguridad de la Información y por tanto deben seguir los lineamientos de gestión enmarcados en esta política y en los estándares, normas, guías y procedimientos recomendados por el Comité de Seguridad de la Información y aprobados por los directivos.

2.1 Roles y responsabilidades de la seguridad de la información.

En cumplimiento a la normativa externa e interna aplicable, la administración de la seguridad de la información institucional de la UPMP, corre a cargo del siguiente grupo de servidores públicos:

1. **Rectoría, Es el único en autorizar el respaldo de la información**, las medidas y las acciones que marca este documento.
2. El Responsable de Seguridad de la Información Institucional (RSII), es responsable del cumplimiento de las normativas aplicables a la seguridad de la Información de la Institución.
3. El Grupo Estratégico de Segridad de la Información (GESI) debe atender oportunamente la formación de los grupos y equipos necesarios para hacer cumplir las funciones establecidas en el proceso de Administración de la Seguridad de la Información (ASI) y en el Proceso de Operación de los Controles de Seguridad (OPEC).

4. El Jefe de Departamento de Servicios Informáticos, es responsable de asegurar la alineación operativa de TIC a la normativa aplicable en materia de seguridad de la Información.
5. Las direcciones de Recursos Materiales y Jurídico, deberán asegurarse de que los contratos de prestación de servicios TIC, cuente con cláusulas que promuevan el cumplimiento de esta política.
6. Los mandos medios y superiores de las áreas de los procesos sustantivos y de apoyo, son responsables de la observancia y cumplimiento de estas Políticas Generales de Seguridad de la Información.
7. Todos los colaboradores en general que presten sus servicios a UPMP, son responsables de conocer y cumplir las Políticas de este manual que les corresponda.

2.2 Responsabilidades de los estudiantes.

Para poder usar los recursos de TI de la Universidad, los estudiantes deben leer y aceptar en cada matrícula de cuatrimestre un acuerdo con los términos y condiciones. El jefe de oficina de soporte técnico de Sistemas debe asegurar los mecanismos para la difusión y aceptación de dichas condiciones por medio de registros y manuales en línea.

El estatuto estudiantil debe contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones.

2.3 Responsabilidades de Usuarios Externos

Todos los usuarios externos y personal de empresas externas deben estar autorizados por unmiembro del personal de la Universidad quien será responsable del control y vigilancia del uso adecuado de la información y los recursos de TI institucionales. Los procedimientos para el registro de tales usuarios deben ser creado y mantenido por la Oficina Asesora de Sistemas en conjunto con la Red de Datos UDNET y la Oficina de Recursos Humanos.

Los usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de TI institucionales. Las cuentas de usuarios externos deben ser de perfiles específicos y tener caducidad no superior a ***tres (3) meses***, renovables de acuerdo a la naturaleza del usuario.

2.4 Usuarios invitados y servicios de acceso público.

El acceso de usuarios no registrados solo debe ser permitido al sitio web de información institucional. El acceso y uso a cualquier otro tipo de recurso de información y TI no es permitido a usuarios invitados o no registrados.

3. Política de Seguridad de la Información.

3.1 Definición de la Política General de Seguridad de la Información.

La información es un recurso que, como el resto de los activos, tiene valor para la institución y por consiguiente debe ser debidamente protegida.

El establecimiento, seguimiento, mejora continua y aplicación de la Política de Seguridad de la Información garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas. Con esta política se contribuye a minimizar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones sustantivas de la entidad apoyadas en un correcto sistema de información.

La institución establecerá los mecanismos para respaldar la difusión, estudio, actualización y consolidación tanto de la presente política como de los demás componentes del Sistema de Gestión de la Seguridad de la Información y alinearlos de forma efectiva con los demás sistemas de gestión.

"La UPMP reconoce que la información de su propiedad y la de sus clientes, así como, los activos de información y la infraestructura que la soporta, son esenciales para la continuidad del negocio y para el cumplimiento de su misión y su visión; por lo que es fundamental protegerlos, restringiendo el acceso, uso y revelación, conforme a sus intereses institucionales".

3.2 Políticas Generales de Seguridad de Información.

1. Rectoría debe asegurarse de que existan los recursos humanos, materiales y tecnológicos para implementar planes y programas en aspectos de seguridad de la información.

2. La Dirección General debe nombrar un Responsable de Seguridad de la Información Institucional (RSII).

3. El RSII debe establecer un Grupo Estratégico de Seguridad de la Información (GESI), que será responsable de implantar y mantener un Sistema de Gestión de la Seguridad de la Información (SGSI).

4. El RSII debe coordinar la revisión anual del cumplimiento de los objetivos y las métricas de seguridad de la información.

5. El RSII, a través del GESI, debe verificar que se definan e implementen controles que se deriven de este Manual de Políticas de Seguridad.

6. La Direcciones Generales Adjuntas, deben alinear sus procesos de gestión y operación, a este Manual de Políticas Generales de Seguridad de la Información.

7. El RSII, debe verificar que se desarrolle y cumpla la implementación de controles del Sistema de Gestión de Seguridad de la Información.

3.3 Revisión de la Política General de Seguridad de la Información.

En este documento se establecen las Políticas Generales de Seguridad de la Información, que tienen efecto inmediato a partir de la fecha de su autorización y publicación, con vigencia permanente o hasta la publicación de una nueva versión, la revisión mínima debe ser de manera anual, que como resultado de la misma sea pertinente para cumplir las necesidades de la Institución en materia de seguridad de la información.

3.4 Conocimiento de la Política General de Seguridad de la Información de la Universidad Politécnica Metropolitana de Puebla.

El Manual de Políticas Generales de Seguridad de la Información de la UPMP, es un documento de carácter normativo, por lo que es fundamental difusión entre todos los colaboradores de la Institución, para su conocimiento.

4. Organización para la seguridad de la información.

4.1 Responsabilidad

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Universidad Politécnica Metropolitana de Puebla, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

Las directivas institucionales aprueban esta Política y son responsables de la autorización de sus modificaciones.

El **Comité de Seguridad de la Información** de la institución es responsable de revisar y proponer a las directivas institucionales para su aprobación, el texto de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad de la institución. Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad de la información al interior de la Universidad.

El **Coordinador del Comité de Seguridad de la Información** será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política.

El **grupo responsable de Seguridad Informática** será responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la entidad, lo cual incluye la operación del SGCI y supervisión del cumplimiento, dentro de la dependencia, de aspectos inherentes a los temas tratados en la presente Política. El nivel de supervisión que pueda realizar cada grupo responsable de seguridad, está relacionado con el talento humano que lo conforma y en todo caso deberá ser aprobado por el Comité de Seguridad de la Información.

Los **propietarios de activos de información (ver su definición en el glosario)** son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la

información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

El **jefe de Recursos Humanos** cumplirá la función de notificar a todo el personal que se vincula contractualmente con la Universidad, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los *Compromisos de Confidencialidad* y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el Comite de Seguridad de la Información.

El **jefe de la Oficina de soporte ténico** en coordinación con el **Jefe de Departamento de Servicios Informáticos** deben seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información y los recursos de tecnología de esta casa de estudios.

Corresponde a dichas jefaturas determinar el inventario de activos de información y recursos tecnológicos de los cuales son propietarios o custodios, el cual será revisado y avalado por el **Jefe de Oficina de Soporte Técnico** y el **Jefe de Departamento de Servicios Informáticos.**

El Abogado General de nuestra institución verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con empleados y con terceros. Asimismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la Información vigente.

La O**ficina de Control Interno** es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información. Es su responsabilidad informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

5. Gestión de activos.

Cada dependencia, bajo supervisión del Comité de Seguridad de la Información, debe elaborar y mantener un inventario de los activos de información que poseen (procesada y producida). Las características del inventario, donde se incorpore la clasificación, valoración, ubicación y acceso de la información, las especifica el **Comité de Seguridad de la Información,** correspondiendo a la **Oficina Asesora de Sistemas** brindar herramientas que permitan la administración del inventario por cada dependencia, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.
En coordinación con la **División de Recursos Físicos** y la **Sección de Almacén** tienen la

responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la institución.

5 Seguridad de la información en el Recurso Humano

Asegurar la protección de la información institucional y de los activos de información que la contengan.

5.1 Inventario de Activos.

Un activo de información, es un elemento reconocible que almacena datos, registros, información en cualquier medio y que tiene las características siguientes:

1. Es valioso para la UPMP por la información que contiene.
2. No es de fácil reemplazo y en algunos casos pudiera ser irrepetible.

Es responsabilidad de los mandos medios y superiores de las áreas de cada dirección de la UPMP identificar sus activos de información.
El Departamento de Servicios Informáticos, debe mantener un registro actualizado sobre los activos informáticos que soporten los servicios TIC de la UPMP.El GESI debe coordinar la identificación de los activos esenciales de la Institución y promover su protección de estos activos.

5.2 Propiedad de los activos.

Toda información que se genere a partir de un activo propio, arrendado o contratado por un servicio, es propiedad de UPMP y quien la resguarda, se convierte en responsable de la misma.

Todo activo de información debe ser asignado a un responsable y autorizado por su jefe inmediato.

La persona responsable del activo debe:

1. Salvaguardar la integridad, disponibilidad y confidencialidad del activo.
2. Hacer uso del activo únicamente para los propósitos y actividades de la Institución.
3. Reportar cualquier incidente o problema relacionado con el activo de información.
4. Cualquier omisión (con dolo o involuntaria) de reportar algún incidente relacionado a cualquier activo bajo su guarda y custodia, se considera una falta hacia la seguridad de la información que en su caso deberá de ser informado a las autoridades competentes.
5. Realizar lo necesario para mantener el activo de información en buenas condiciones que garanticen y cumplan su función.

5.3 Uso aceptable de los activos.

UPMP considera que los recursos para el procesamiento de la información son prioritarios para el desarrollo de los procesos de negocio y el adecuado cumplimiento de sus funciones;

por lo que, es responsabilidad del personal, el salvaguardar de cualquier alteración o modificación no autorizada, daño o destrucción que límite su disponibilidad para el adecuado desarrollo de sus actividades.

El uso aceptable de los activos de información incluye:

1. vitar daños temporales o permanentes a los activos de información, causados por accidentes, imprudencias o daños dolosos.
2. Reportar cualquier falla o mal funcionamiento detectado.
3. Informar a los jefes inmediatos, de cualquier falla o vulnerabilidad de los activos de información.
4. Notificar de cualquier necesidad de protección o mejora, en los controles para los activos de información.
5. Usar los activos de información únicamente para los propósitos de la Institución.
6. Reportar cualquier uso no adecuado del activo de información a su jefe inmediato.

5.4 Devolución de activos.

Todo personal que preste sus servicios a UPMP, al concluir sus funciones, tiene la obligación de entregar los activos informáticos asignados en buen estado físico y de operación, así como los activos de información y la documentación correspondiente.

6. Clasificación de la información.

6.1 Directrices de clasificación.

Cada área debe clasificar y etiquetar su información de acuerdo a la Ley Federal de Transparencia y Acceso a la Información Pública.

La información debe clasificarse como:

1. **Información reservada:** es la información creada y usada por UPMP, en la realización de sus procesos, que corresponda a lo dispuesto en la Ley Federal de Transparencia y Acceso a la Información Pública.
2. **Información confidencial**: es la información creada y usada por UPMP, en la realización de sus procesos de la Ley Federal de Transparencia y Acceso a la Información Pública. El acceso a esta información es restringido y debe resguardarse con los niveles más altos de integridad, confidencialidad y disponibilidad restringida. Su divulgación externa debe estar en apego a los términos de las disposiciones aplicables.
3. **Información pública:** toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados en el ámbito federal, es pública, accesible a cualquier persona y sólo podrá ser clasificada excepcionalmente como reservada o confidencial, en términos de la Ley Federal de Transparencia y Acceso a la Información.

Toda información de la Institución debe tener un responsable designado por un mando medio o superior para su resguardo, para asegurar que las medidas de protección sean

puestas en práctica y así salvaguardar la integridad, confidencialidad y disponibilidad de la información. En caso de que se solicite información a través de la Ley de Transparencia, la Unidad Administrativa debe solicitar la clasificación de información al Comité de Transparencia.

6.2 Etiquetado de la información.

La información clasificada como reservada o confidencial, debe ser confirmada por el Comité de Transparencia, y debe contener la leyenda de "clasificación" de conformidad con las disposiciones aplicables. El etiquetado de la información, se aplica sólo para la información reservada.

6.3 Protección y manejo de la información.

1. El Departamento de Servicios Informáticos y el Departamento de Recursos Materiales deben proveer mecanismos de protección de la información, de acuerdo a su clasificación.
2. Todo activo de información protegido debe contar con un control de acceso formal, donde establezca que personas son autorizadas para el manejo de la información.
3. La información debe respaldarse en un nivel de protección consistente con su clasificación.
4. Los funcionarios están obligados a no revelar a terceras personas la información que conozcan por el ejercicio de sus funciones, por lo que están obligados a mantenerla confidencial y privada para evitar su divulgación.
5. Los usuarios de acuerdo a sus funciones podrán trabajar y hacer uso de la información institucional en los activos de información asignados y resguardar la versión final.

7. De la Seguridad física y lógica

SEGURIDAD FÍSICA. Para la Universidad a el mantener la integridad y confiablidad de los espaci os físicos donde se encuentre albergado cualquier elemento de información que tiene val or para la institución, o es necesario para mantener la continuidad de las operaciones de l a mi sma y los recursos de los si stemas de información, la infraestructura de telecomunicaciones, la infraestructura de energía eléctrica, equipo de cóm puto, cli mas, si stemas de almacenamiento y dispositivos periféricos , entre otros, para lograrl o se deberá observar l o si guiente:

- Prevenir e impedir el acceso no autorizado a áreas e instalaciones restringidas;
- Establecer medidas de seguridad para proteger la información en las áreas de trabajo;
- Prevenir el daño e interferencia a las áreas, in stalaciones y recursos fisi cos de la Universidad provocados por fenómenos ambientales, sociales y fallos en l a infraestructura; y
- Preservar los acti vos de información TIC utilizados para el tratamiento de información de la Universidad, entendido como la captura, procesamiento, transferencia, almacenamiento y destrucción de información.

2 SEGURIDAD LÓGICA. Dentro de la Universidad la mayoría de los daños que puede sufrir cualq u ier elemento que tiene va lor para la institución, o es necesario para mantener la continuid ad de l as operaciones de l a misma, no será sobre los medios físi cos sino contra la información almacenada. Por l o que deben existir técnicas que la protejan, resguardando el acceso a los datos, y restringiendo su acceso sólo a los usuarios autorizados para hacerlo, para lo cual deberá

observarse lo siguiente:

- Todo usuario debe firmar el compromiso de confidencialidad de la información que tiene a su disposición o de que conoce, con motivo del desempeño de su función;

- La información que se encuentre protegida por derechos de autor que sea titularidad de terceros o propiedad de la Universidad, deberá utilizarse con apego a la legislación en la materia;

- Establecer controles que garanticen la seguridad de la transferencia de información y el uso de los recursos del conjunto de tecnologías apl icadas para proveer a las personas de la información y comunicación a través de medios tecnológicos de última generación;

- Instaurar procedimientos de respaldo y recuperación de la información institucional, la cual será resguardada periódicamente para garanti zar su identificación, protección, integridad y disponibilidad; y

- Cualquier medio que deba desecharse y que contenga información institucional, deberá destruirse o apli cársel e un método de borrado seguro, que evite el acceso a la misma o su recuperación posterior, atendiendo a las disposiciones norm ativa s establecidas en la institución.

7.1 *Seguridad física y ambiental.*

7.1.1 Areas seguras.

Perímetro de seguridad física

El RSII, a través de El Departamento de Servicios Informáticos y en conjunto con el Departamento de Recursos Materiales, debe informar al GESI la designación de las áreas seguras de la Institución.

Recursos Materiales y la de Servicios Informáticos son responsables de definir un espacio físico seguro, que cumpla con lo mínimo para asegurar el procesamiento y almacenamiento de la información.

Se deberán de implementar los mecanismos necesarios que permitan limitar el acceso a las áreas seguras, solamente para el personal autorizado

No se permitirá el acceso a las áreas seguras al personal que no esté expresamente autorizado. Es responsabilidad de las personas autorizadas a las áreas restringidas, permitir el acceso al
personal ajeno a éstas.

Control físico de entrada

Las áreas seguras deben contar con mecanismos de ingreso que consideren la autorización, registro y validación de los accesos.

Seguridad de oficinas, despachos y recursos

La Dirección de Recursos Materiales debe proporcionar a cada empleado un espacio físico asignado que cuente con mobiliario protegido para el resguardo de información física.

La Dirección de Recursos Materiales debe proporcionar a cada empleado un acceso controlado para el uso de las instalaciones de acuerdo a sus funciones dentro de la Institución, el acceso a áreas restringidas debe ser autorizado por la dirección responsable

del área restringida.

Protección contra amenazas externas y ambientales

La Dirección de Recursos Materiales debe facilitar los recursos necesarios para establecer perímetros de seguridad física con el fin de proteger áreas que contengan información crítica de la Institución, así como el área de procesamiento de datos.

Los perímetros de seguridad física deben estar bien definidos e identificados, esto depende del valor de los activos de información a proteger.

El perímetro de seguridad física de los centros de cómputo de UPMP, debe considerar los requerimientos definidos en el Manual de Políticas y Procedimientos para los Recursos Materiales y Servicios Generales en UPMP.

El trabajo en áreas seguras

Las áreas de acceso a las instalaciones de UPMP, deben ser controladas y debe restringirse el acceso a las áreas seguras para evitar el acceso no autorizado.

7.2 *Seguridad de los equipos.*

Ubicación y protección de equipos

Todo equipo que almacene, procese o transmita información esencial para la operación de UPMP, debe ser protegido para disminuir el riego de amenazas ambientales o físicas; tales como, inundaciones, rayos, sismos, radiaciones, polvo, humedad, vandalismo, explosión, humo etc.

La Institución debe contar con un centro de datos primario, que garantice la protección de los equipos que soportan los procesos institucionales, así como, los servicios de soporte.

Además, debe contar con un centro de datos secundario, que garantice la integridad, confidencialidad, disponibilidad de la información y cuya ubicación geográfica sea diferente del centro de datos primario, que garantice la continuidad de las operaciones, ante una contingencia.

Todos los equipos de soporte que se encuentran fuera de los centros de datos, deben estar ubicados y protegidos en áreas restringidas, de acuerdo a las especificaciones del fabricante.

Para lo anterior, El Departamento de Servicios Informáticos debe considerar:

- Que ambos centros de datos, principal y secundario, cumplan con los estándares internacionales y con la norma mexicana “Centros de Datos de Alto Desempeño Sustentable y Energético – Requisitos y Métodos de Comprobación”.
- Que ambos centros de datos, principal y secundario, consideren los estándares mínimos para la protección física y ambiental; siguiendo las Directrices de Seguridad de Cómputo Institucional.

Para los centros de datos de UPMP debe estar provisto como mínimo de:

- Señalización adecuada de todos los equipos y elementos de seguridad, como luces de emergencia, etc.; que establezcan las normas de seguridad industrial y de salud ocupacional.

- Sistemas de aire acondicionado de precisión redundante y adecuada, para garantizar una temperatura idónea para el correcto funcionamiento de los equipos y prevenir fallas.
- Unidades de alimentación ininterrumpida (UPS), redundante.
- Alarmas de detección de humo y sistemas automáticos de extinción de fuego.
- Extintores y equipo contra incendio con capacidad de detener el fuego generado por equipo eléctrico.
- Contar con un control de acceso sólo para personal autorizado.

Instalaciones de suministro

Las instalaciones de procesamiento de información que opera la Institución, deben contar con equipos que suministren de energía eléctrica de forma ininterrumpida por al menos 24 horas, tales como generadores y UPS, así como, sus procedimientos documentados en caso de contingencia.

Seguridad en cableado

El cableado debe cumplir con las especificaciones del fabricante para minimizar errores físicos. No debe estar expuesto a condiciones ambientales que aceleren su deterioro, tales como: agua, corrosivos, exceso de calor, etc.

Todo el cableado de datos debe estar debidamente etiquetado en los paneles de parcheo y adecuadamente instalado, para facilitar su mantenimiento. Cuando exista un cambio en el cableado, se debe actualizar la memoria técnica correspondiente.

El cableado de datos y de energía debe estar separado en distintitas canaletas o ductos, para evitar interferencias, siguiendo las normas aplicables.

El acceso a los cuartos donde residan los paneles de parcheo y tableros de distribución eléctrica, deben ser restringido al personal responsable de la red y del soporte técnico o mantenimiento de la misma.

Mantenimiento de los equipos

Todo activo de información debe contar con programas de soporte y mantenimiento, para asegurar su correcto funcionamiento y garantizar su disponibilidad.

El Departamento de Servicios Informáticos debe validar que los mantenimientos que se lleven a cabo, sean realizados por personal capacitado, de acuerdo a las especificaciones del fabricante. Asimismo, asegurarse que se conserve un registro de todos los mantenimientos preventivos y correctivos efectuados.

Salida de activos

El Departamento de Servicios Informáticosen coordinación con la Departamento de Servicios Generalesdebe establecer un procedimiento para el registro de entrada y salida de equipo de cómputo fuera de las instalaciones de UPMP.

Seguridad de los equipos y activos fuera de las instalaciones

Todo equipo que almacene, procese, transmita información crítica de UPMP debe operar

dentro de las instalaciones de la Institución o de las contratadas para tal efecto o por fuerzas de causas mayores ajenas a la institución en caso de una contingencia se podrán prestar los equipos.

Los equipos que por necesidad salgan de las instalaciones de UPMP sean propias o arrendadas, deben apegarse al procedimiento de salida de equipos que se encuentra como anexo en el Manual de Políticas y Procedimientos para los Recursos Materiales y Servicios Generales en UPMP, así como firmar un formato de confidencialidad de la información.

El Departamento de Servcios Informáticos debe establecer un procedimiento que asegure que la información y/o configuraciones no queden expuestas.

Los equipos de cómputo móviles (laptops) de UPMP deben ser protegidos con las medidas y mecanismos de seguridad de la información, con los que cuente la Institución.

Los equipos de cómputo móviles (laptops) de UPMP que se encuentran fuera de las instalaciones y requieran conectarse a la red interna de UPMP solo podrán realizarlo por medio del cliente de VPN institucional.

Reutilización o baja de dispositivos de almacenamiento

El Departamento de Servicios Informáticos debe implementar un proceso de baja o devolución que garantice el borrado seguro de los activos de información y notificar al RSII para su verificación.

Equipo informático de usuario desatendido

El Departamento de Servicios Informáticos debe implementar en todo equipo informático las configuraciones necesarias para su bloqueo de forma automática, una vez que éste se encuentre desatendido.

Política de escritorio seguro y bloqueo de pantalla

Todo el personal que preste sus servicios dentro de UPMP, debe cumplir con los siguientes lineamientos al ausentarse de su lugar de trabajo o finalizar su jornada laboral:

- En caso de contar con puerta, cajones o archiveros, éstos deben cerrarlos con llave.
- Retirar del escritorio cualquier tipo de información, sin importar el medio en que se encuentre (papel, post-its, discos, medios magnéticos) y resguardarla en gabinetes con llave o cualquier otro mueble con acceso controlado.
- Destruir de manera segura aquella información que ya no será utilizada.
- No dejar documentos con información sobre impresoras, copiadoras, etc.
- No utilizar la información impresa que sea confidencial o de uso restringido para reciclaje.

7.3 *Protección contra Código malicioso.*

Controles contra el código malicioso

Departamento de Servicios Informáticos debe asegurar que todos los equipos de escritorio, móviles (laptops) y servidores utilizados en la red de la Institución, tengan instalado el software antivirus, anti-malware, anti-xploits, anti-spam y anti-spyware institucional y mantenerlo actualizado, tanto en versión como en definición de firmas. Así mismo, deben cumplir con una configuración base de parches de seguridad.

Los proveedores o personal externo que tengan equipos y que necesiten conectarse a la red de la Institución, deben contar con un software de antivirus autorizado por la Departamento de Servicios Informáticos.

El software de antivirus anti-malware, anti-xploits, anti-spam y anti-spyware institucional debe permitir como mínimo:

1. Ejecutar búsqueda automática, manual o programable.
2. Limpiar archivos infectados.
3. Mantener en cuarentena los archivos que no puedan ser limpiados.
4. Contar con mecanismos para prevenir y contener amenazas, así como, negación de servicios.
5. Proveer la capacidad de actualizaciones automáticas y programables.
6. Registrar los incidentes de virus y contar con la capacidad de análisis de registro.
7. Detectar código malicioso.
8. Generar alertas.
9. Llevar una administración centralizada.

El software contra código malicioso y sus componentes deben ser actualizados cuando exista una nueva versión o definición de firmas, con base a los contratos con el fabricante.

Departamento de Servicios Informáticos debe dar acceso al RSII al repositorio de los reportes mensuales detallando las incidencias detectadas por el antivirus.

7.4 *Respaldo y borrado de información.*

Respaldo de información

Todos los mandos medios y superiores de las áreas dentro de la Institución son responsables de identificar la información que sea sensible para la operación de su área de acuerdo a su criticidad y deben dar aviso a Departamento de Servicios Informáticos para gestionar su respaldo y periodicidad.

Departamento de Servicios Informáticos debe:

1. Implementar procedimientos para respaldar la información de la Institución.
2. Respaldar periódicamente toda la información (configuraciones, logs, file systems, bases de datos, etc.) que resida en los sistemas de la Institución, considerando su criticidad.

3. Asegurar que el respaldo de la información de los sistemas, en lo posible no degrade su operación.
4. Los respaldos deben llevarse a cabo preferentemente fuera de los horarios de operación y se documentan las excepciones.
5. Proveer espacios suficientes para almacenamiento y resguardo de la información del negocio que será respaldada periódicamente, siendo responsabilidad de cada usuario el manejo de la información a respaldar.
6. Revisar y validar periódicamente la información respaldada, para evitar que se pierda, se vuelva obsoleta o se deteriore; asegurando que la información sea recuperable y que cumple con los principios de integridad y disponibilidad.
7. Evitar que los medios de respaldo utilizados para el almacenamiento de información se vuelvan obsoletos. En la medida de lo posible, debe utilizar tecnologías de punta que permitan reducir el espacio físico que ocupan estos medios.
8. Almacenar los respaldos generados en un sitio protegido contra el medio ambiente y con controles estrictos de acceso, que debe ubicarse a una distancia razonable fuera del alcance de un evento en la zona principal.
9. Mantener un registro actualizado, con acceso controlado, que contenga los datos de todos los archivos respaldados, fuera de las instalaciones de la Institución, indicando la fecha más reciente en que la información fue modificada y la naturaleza de la misma.

Restauración e integridad

El Departamento de Servicios Informáticos debe implementar medidas y procedimientos para garantizar la integridad y disponibilidad de la información de la Institución que sea respaldada.

El Departamento de Servicios Informáticos debe:

1. Garantizar que los respaldos no sean alterados.
2. Garantizar la integridad, disponibilidad y confidencialidad de los respaldos por lo menos cinco años, desde su último respaldo.
3. Realizar pruebas programadas y documentadas de restauración de información, simulando situaciones de contingencia, bajo parámetros de tiempo establecidos, en donde se revise la integridad y funcionalidad de los respaldos de información reportando los resultados al RSII.

Almacenamiento de información

El Departamento de Servicios Informáticos debe proporcionar y administrar espacio de almacenamiento suficiente para que las áreas puedan resguardar copia de su información institucional. Asimismo, debe contar con un inventario de usuarios autorizados en los recursos de almacenamiento de cada área.

Queda prohibido la utilización de recursos de almacenamiento institucional para archivos de uso personal o de diversión.

El Departamento de Servicios Informáticos debe contar con procedimientos y mecanismos de borrado o destrucción y de la información de la Institución, que ya no sea necesaria, ni por la operación, ni por requerimientos legales.

Toda la información que ya no sea utilizada se debe eliminar de forma segura, de acuerdo a los criterios que establezcan las áreas responsables de la información.

7.5 *Registro de Actividad.*

Registro de eventos

Todos los sistemas y aplicaciones críticos de la Institución, bases de datos y dispositivos de red y servidores, deben contar con registros de eventos y bitácoras de seguridad protegidos debidamente.

El Departamento de Servicios Informáticos debe resguardar por un periodo de al menos tres años todos los registros de incidentes, alarmas, cambios, configuraciones, entre otros, que deben estar disponibles para su extracción y revisión por parte del RSII, cuando sean requeridos.

La Dirección de Tecnologías de Información y Comunicaciones, debe asegurar que los registros de acceso a sistemas, bitácoras, bases de datos y cualquier otro registro de seguridad de los aplicativos; se almacenen en un repositorio accesible para cualquier tipo de revisión o análisis.

Protección de la información de los registros

Responsable de la Seguridad de la Información, debe validar que se implementen controles para la generación y conservación de bitácoras de seguridad, para los sistemas identificados como parte de una infraestructura esencial.

En estas bitácoras se debe registrar el usuario, nombre de equipo, dirección IP, hora de entrada y salida del sistema, así como, el tipo de consulta o cambios realizados en la configuración de las aplicaciones. Estas bitácoras deben tener un tiempo mínimo de almacenamiento de 90 días en línea.

Los controles que se implanten para proteger estos registros, deben incluir protección contra modificaciones, daños, mal uso o corrupción de los datos.

Registro del administrador y el operador

El Departamento de Servicios Informáticos debe contar con un registro de las actividades de los operadores y administradores de los sistemas. Éstos deben incluir como mínimo lo siguiente:

1. El tiempo en que ocurrió el evento.
2. Detalles del evento o fallas en el mismo.
3. Detalles de la cuenta de usuario y/o administrador implicado.

Sincronización de reloj

Todos los equipos de cómputo, sistemas, servidores, bases de datos y de comunicaciones que se encuentren en los dominios de red de la Institución, deben estar sincronizados con una fuente común y exacta de tiempo (servidor NTP).

El Departamento de Servicios Informáticosy las áreas de negocio con contratos de servicios con terceros, deben implementar y documentar procedimientos para que los cambios de horario no afecten la operación de la Institución.

Todos los equipos de cómputo y comunicaciones deben configurarse para que se sincronicen con el servidor NTP.

7.6 *Control de Software en sistemas operacionales.*

Instalación de software

El Departamento de Servicios Informáticos debe contar con procedimientos para la certificación y validación del software que sea instalado. Asimismo, debe asegurarse que todo el software que se instale en los servidores y equipos de cómputo personal cuente con el licenciamiento vigente, suficiente para atender los requerimientos del negocio.

El Departamento de Servicios Informáticos es responsable de administrar y resguardar las licencias del software institucional.

Todo el software que se instale en ambientes productivos debe ser previamente evaluado y probado en ambientes de pruebas. La instalación del software autorizado debe ser realizada por personal experto, siguiendo los lineamientos de control de cambios y llevando un control estricto de las versiones.

Todo el software que se instale en los equipos de cómputo personal de UPMP debe estar inventariado en un catálogo de software institucional. Es responsabilidad de El Departamento de Servicios Informáticosgestionar la adquisición del software requerido por las áreas de negocio.

El Departamento de Servicios Informáticoses la única instancia autorizada para instalar, actualizar y desinstalar el software de los equipos de cómputo.

El Departamento de Servicios Informáticos debe contar con procedimientos para la certificación y validación del software que sea instalado. Asimismo, debe asegurarse que todo el software que se instale en los servidores y equipos de cómputo personal cuente con el licenciamiento vigente, suficiente para atender los requerimientos.

7.7 *Gestión de la vulnerabilidad técnica.*

Gestión de las vulnerabilidades

La Institución a través de El Departamento de Servicios Informáticos y la Dirección de Contraloría Interna deben establecer el alcance de las evaluaciones que se realicen para identificar vulnerabilidades en el hardware, software, sistemas, aplicaciones, seguridad, recuperación de información y redes.

Departamento de Servicios Informáticos debe coordinar la realización de los análisis de vulnerabilidades con una metodología que certifique las pruebas de caja gris y caja negra y disminuir el riesgo por falta de disponibilidad.

El RSII, a través de responsable de la Seguridad de la Información, debe documentar el seguimiento a las acciones de mejora, para solventar las vulnerabilidades detectadas, siguiendo el plan de remediación propuesto por la Dirección de Tecnologías de Información y Comunicaciones.

Las restricciones a la instalación de software

Queda prohibido al personal no autorizado instalar y/o ejecutar software para explorar

(escanear) redes, equipos de cómputo y sistemas de información, en busca de protocolos, puertos, recursos compartidos y vulnerabilidades; así como, el descubrimiento y monitoreo no autorizado del tráfico de la red de la Institución. El Departamento de Servicios Informáticos debe implementar mecanismos para restringir la instalación de software no autorizado.

8. Seguridad de las Comunicaciones.

Controles de red

El Departamento de Servicios Informáticoses responsable del diseño, implementación, establecimiento, contratación, administración, mantenimiento y soporte de las redes de voz y datos y de toda la infraestructura de comunicaciones que las soportan.

El Departamento de Servicios Informáticos debe implementar procedimientos y controles de seguridad que garanticen la integridad, disponibilidad y confidencialidad de la información, en su transmisión en las redes e infraestructuras de comunicaciones de la Institución.

El Departamento de Servicios Informáticos debe establecer los requerimientos técnicos para la conexión a la red y sus servicios.

UPMP debe contar con la infraestructura necesaria para la protección de la información y sus activos tecnológicos, así como, para el monitoreo y detección oportuna de incidentes de seguridad.

El Departamento de Servicios Informáticos debe implementar mecanismos para el uso del servicio de internet en la Institución, el cual debe contar con herramientas de seguridad y de filtrado de contenido, búsquedas e imágenes en internet, que permitan la segmentación del mismo en distintas categorías, reportes y soporte de sitios de nueva generación y/o micro-aplicaciones.

El Departamento de Servicios Informáticos debe proteger la información que de estos servicios que se deriven, mediante la correcta configuración de los servidores y/o dispositivos sobre los que operan estos servicios.

Seguridad de los servicios de red

La Dirección de Tecnologías de Información debe implementar:

- Mecanismos que midan y aseguren niveles de disponibilidad y tiempos de respuesta, que garanticen la adecuada ejecución de las operaciones y servicios bancarios que se realizan.
- Medidas de control que garanticen la protección, seguridad y confidencialidad de la información, generada por la realización de operaciones bancarias, a través de cualquier medio tecnológico.

La Seguridad de la Información, debe llevar a cabo revisiones periódicas de conexiones externas, tomando en consideración los siguientes puntos:

1. Vigencia
2. Dueño de la conexión externa por parte de la Institución
3. Descripción de la conexión externa
4. Uso de la conexión externa

5. Arquitectura de seguridad

Los tipos de conexiones externas que se pueden permitir son las siguientes:

- Conexiones con instalaciones de la Institución que no están integradas a la red interna
- Conexiones con otras entidades financieras
- Conexiones con proveedores
- Conexiones públicas
- Conexiones a través de Redes Privadas Virtuales (VPN).

Se pueden establecer redes abiertas, únicamente al proporcionar servicios a la población, las cuales deben estar separadas y aisladas de la red de datos.

9. Infracciones a la politica de Seguridad.

Las acciones que se enumeran a continuación, en manera enunciativa más no limitativa, constituyen infracciones a la Política de Seguridad de UPMP.

1. **Son acciones de falta u omisión a las Políticas Generales de Seguridad de la Información:**

   a) No firmar los acuerdos de confidencialidad o de responsabilidad de activos de información.

   b) No actualizar la información de los activos de información a su cargo.

   c) No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ellos.

   d) No guardar de forma segura la información cuando se ausente de su puesto de trabajo o al terminar la jornada laboral.

   e) Dejar información en carpetas compartidas, no autorizadas o en lugares distintos al servidor de archivos institucional, obviando las medidas de seguridad.

   f) Dejar las gavetas abiertas o con las llaves puestas en los escritorios.

   g) Permitir que personas ajenas a la Institución, deambulen sin acompañamiento en el interior de las instalaciones, en áreas no destinadas al público.

   h) Solicitar cambio de contraseña de otro usuario.

   i) No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento de UPMP, para traslado, reasignación o para disposición final.

   j) Utilizar claves de acceso de un usuario distinto al propio para ingresar a los sistemas y/o aplicativos.

2. **Son acciones de mal uso de la plataforma tecnológica institucional:**

   a) Hacer uso de la red de datos institucional, para acceder, almacenar, mantener o difundir en o desde los equipos institucionales, material con contenido sexual u ofensivo, cadenas de correos y correos masivos no autorizados.

b) La utilización de software no relacionado con la actividad laboral que pueda degradar el desempeño de la plataforma tecnológica institucional.

c) Actuar con negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de UPMP.

d) Conectar equipos de cómputo personal u otros sistemas electrónicos personales a la red de datos institucional, sin la debida autorización.

e) El utilizar los recursos tecnológicos institucionales para beneficio personal.

f) Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por la Dirección de Tecnologías de la Información y Comunicaciones.

3. Son acciones de sabotaje de la plataforma tecnológica institucional:

a) Impedir u obstaculizar el funcionamiento a los aplicativos, bases de datos o a las redes de telecomunicaciones y datos de UPMP, sin estar autorizado.

b) Destruir, dañar, borrar, deteriorar activos informáticos de UPMP, sin autorización.

c) Distribuir, enviar, introducir software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de UPMP.

d) Alterar datos personales de las bases de datos institucionales.

e) Realizar cambios no autorizados en la plataforma tecnológica de UPMP.

4. Son acciones de acceso no autorizado a la infraestructura tecnológica de UPMP:

a) Acceder sin autorización expresa a todo o en parte a los sistemas de UPMP.

b) Suplantar a un usuario ante los sistemas de autenticación y autorización establecidos.

c) No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de UPMP o permitir que otras personas accedan con el usuario y clave del titular a éstos.

d) Otorgar el acceso o privilegios a la infraestructura de UPMP a persona no autorizadas.

e) Ingresar a carpetas sin autorización.

5. Son acciones de robo de información a UPMP:

a) Ejecutar acciones tendientes a eludir o variar los controles establecidos por UPMP.

b) Retirar de las instalaciones de la Institución, estaciones de trabajo o equipos portátiles que contengan información

institucional, sin la autorización pertinente.

c) Sustraer de las instalaciones de UPMP documentos con información institucional, o abandonarlos en lugares públicos o de fácil acceso.

d) Entregar, enseñar y divulgar información institucional, a personas o entidades no autorizadas.

e) Copiar sin autorización los programas de UPMP o violar los derechos de autor o acuerdos de licenciamiento.

Todo personal que identifique la omisión o falta de cualquiera de estas acciones debe hacer del conocimiento a responsable de la Seguridad de la Información quien a su vez informará al RSII, a la Dirección de Recursos Humanos, al Órgano Interno de Control de la falta u omisión de las políticas establecidas en este manual, para que dentro de sus ámbitos de competencias resuelva lo conducente.

9.1 *De la responsabilidad es en caso de Incumplimiento*

Toda persona que haga uso de los activos de información, está obligada a cumplir la presente política de seguridad y los procedimientos aplicables para mantener la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad.

El incumplimiento de las disposiciones citadas en esta política y demás normas en materia de seguridad de la información, dará lugar a la infracción o sanción correspondiente en términos de la legislación universitaria. Cuando la acción implique la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con lo establecido por las normas procesales.

La presente política deberá revisarse al menos una vez al año y entrará en vigor al siguiente día de su aprobación.

REALIZÓ

FERNANDO MIZRAÍM LÓPEZ VÁZQUEZ
JEFE DE DEPARTAMENTO DE SERVICIOS