Política de Seguridad de la Información de la Universidad Veracruzana

TÍTULO I
DISPOSICIONES GENERALES

CAPÍTULO I
DISPOSICIONES GENERALES

1. La presente Política de Seguridad de la Información, tiene por objeto establecer el marco operativo para la seguridad de la información en la Universidad Veracruzana, 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 Veracruzana, 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 Universidad Veracruzana 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.

2. La Universidad Veracruzana, 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.

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

   I. 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 intelectual y, en su caso, a las normas establecidas en la Universidad que resulten aplicables;

II. 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
III. 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.

4. 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.
5. 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.
Proceso. Conjunto organizado de actividades que se llevan a cabo de manera sistemática para producir un bien o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.
Red institucional: Medios de comunicación que se utilicen dentro y hacia la Universidad Veracruzana 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.

CAPÍTULO II
DE LOS OBJETIVOS

6. Definir los mecanismos y controles para salvaguardar cualquier activo de información frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, integridad, disponibilidad y legalidad de la información, estableciendo y vigilando el cumplimiento del marco de actuación general. Observando para ello lo siguiente:

I. Establecer un modelo de gobierno de seguridad en la institución para preservar la integridad, confidencialidad y disponibilidad de los activos de información;
II. Administrar la seguridad de la información, identificando y clasificando cualquier elemento de información que tiene valor para la Universidad, o es necesario para mantener

la continuidad de las operaciones de la misma así como los riesgos y amenazas que enfrenten y que permitan establecer los mecanismos para asegurar la continuidad de los procesos institucionales;

III. Elaborar, establecer, difundir y actualizar las políticas, técnicas y procedimientos que permitan la implementación de las medidas de seguridad correspondientes, para la protección de la información; y

IV. Fomentar una cultura de seguridad de la información en la Universidad Veracruzana para elevar la confiabilidad en el tratamiento de la misma.

TÍTULO II
DE LA SEGURIDAD

CAPÍTULO I
DE LA SEGURIDAD FÍSICA Y LÓGICA

1. SEGURIDAD FÍSICA. Para la Universidad Veracruzana el mantener la integridad y confiablidad de los espacios físicos donde se encuentre albergado cualquier elemento de información que tiene valor para la institución, o es necesario para mantener la continuidad de las operaciones de la misma y los recursos de los sistemas de información, la infraestructura de telecomunicaciones, la infraestructura de energía eléctrica, equipo de cómputo, climas, sistemas de almacenamiento y dispositivos periféricos, entre otros, para lograrlo se deberá observar lo siguiente:

   I. Prevenir e impedir el acceso no autorizado a áreas e instalaciones restringidas;
   II. Establecer medidas de seguridad para proteger la información en las áreas de trabajo;
   III. Prevenir el daño e interferencia a las áreas, instalaciones y recursos físicos de la Universidad provocados por fenómenos ambientales, sociales y fallos en la infraestructura; y
   IV. Preservar los activos 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 Veracruzana la mayoría de los daños que puede sufrir cualquier elemento que tiene valor para la institución, o es necesario para mantener la continuidad de las operaciones de la misma, no será sobre los medios físicos sino contra la información almacenada. Por lo 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:

   I. 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;
   II. 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;
   III. Establecer controles que garanticen la seguridad de la transferencia de información y el uso de los recursos del conjunto de tecnologías aplicadas para proveer a las personas de la información y comunicación a través de medios tecnológicos de última generación;

IV. Instaurar procedimientos de respaldo y recuperación de la información institucional, la cual será resguardada periódicamente para garantizar su identificación, protección, integridad y disponibilidad; y

V. Cualquier medio que deba desecharse y que contenga información institucional, deberá destruirse o aplicársele un método de borrado seguro, que evite el acceso a la misma o su recuperación posterior, atendiendo a las disposiciones normativas establecidas en la institución.

CAPÍTULO II
DEL USO DE LOS ACTIVOS DE INFORMACIÓN

3 El uso de cualquier elemento que tiene valor para la Universidad, o es necesario para mantener la continuidad de las operaciones de la misma, habrán de ser utilizados de forma adecuada para el logro de los fines de la institución y por lo tanto deberán de apegarse a las disposiciones siguientes:

I. Hacer uso ético y legal de los mismos;

II. La Universidad se reserva el derecho de dar acceso a cualquier recurso;

III. Los responsables de administrar los recursos de TIC, deberán establecer y hacer cumplir las medidas necesarias para evitar que estos sean usados para prácticas ilegales o no éticas, ni realizarán acciones que deterioren o pongan en riesgo su desempeño, y cualquier actividad que implique un uso excesivo de ellos, deberá previamente ser autorizada por los responsables de administrar dichos recursos y realizarse en ambientes controlados; y

IV. No podrán ser utilizados para uso privado y comercial.

CAPÍTULO III
DE LOS RESPONSABLES DE LA APLICACIÓN

4 Los responsables de dar seguimiento y cumplimiento a las disposiciones establecidas en la presente políticas son:

I. **Comité para la Seguridad Informática de los Datos Personales de la Universidad Veracruzana:** Órgano responsable de analizar y establecer las medidas de seguridad requeridas en materia de protección de datos personales en sistemas informáticos indicadas por la Ley 581 para la Tutela de los Datos Personales en el Estado de Veracruz de Ignacio de la Llave; así como aprobar la política, objetivos y programa de seguridad informática de los mismos en la Institución;

II. **Responsables de los Sistemas de Datos Personales:** En las entidades académicas y dependencias de la Universidad, son los responsables de los ficheros, que son los registros de datos personales que se requieran para controlar las entradas y salidas de los recursos de TIC de un edificio, o base de datos, entendido estas como el conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso, con datos de carácter personal. Están obligados a establecer controles y medidas de seguridad para proteger la información bajo su responsabilidad, de acuerdo

a lo establecido en la Ley número 581 para la tutela de los datos personales para el Estado de Veracruz de Ignacio de la Llave;

III. **Encargado del tratamiento de los Datos Personales:** Es toda aquella persona que en el servicio de sus atribuciones, realiza tratamiento de datos personales de forma cotidiana;

IV. **Dirección General de Tecnología de Información:** Es responsable de diseñar y aprobar el programa de medidas técnicas de seguridad, necesarias para proteger los activos de información de la institución, evitando su alteración, pérdida, comercialización, transmisión y acceso no autorizado, así como proponer al Comité para la Seguridad Informática de los Datos Personales de la Universidad Veracruzana, la normatividad de seguridad para el acceso y conservación de información almacenada en medios y repositorios institucionales;

V. **Encargados de la administración de equipos de cómputo:** Es responsable de establecer y hacer cumplir, todas aquellas medidas de seguridad para el acceso a los servicios y recursos de TIC que ofrece la entidad académica o dependencia para salvaguardar la integridad, disponibilidad y confidencialidad;

VI. **Grupo de trabajo de Seguridad de la Información:** Se encuentra integrado por representantes de las áreas sustantivas de la Universidad, destinado a la adopción del modelo de gobierno de seguridad de la información, así como su implantación, garantizando el apoyo manifiesto de las autoridades a las iniciativas de seguridad; y

VII. **Dirección General de Recursos Humanos:** Hará llegar el formato de compromiso de confidencialidad a los responsables de las entidades y dependencias de la Universidad Veracruzana, el cual deberá ser suscrito por el trabajador responsable del activo de información; informará la dirección electrónica donde se ubique y contenga la normatividad a observar de esta Política de Seguridad de la Información, manuales, guías, procedimientos y prácticas que de ella deriven y apoyará en las tareas de capacitación continua en materia de seguridad.

CAPÍTULO IV
DE LAS RESPONSABILIDADES EN CASO DE INCUMPLIMIENTO

5 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.

6 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.

7 La Universidad se reserva el derecho a ejercer las acciones legales pertinentes para la protección y defensa de sus legítimos intereses en aquellos supuestos de hecho no directamente contemplados en el presente documento, que sin embargo pudieran tener cabida en el Código Penal o en la legislación vigente.

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

NORMATIVIDAD APLICABLE

1. Constitución Política de los Estados Unidos Mexicanos;
2. Constitución Política para el Estado de Veracruz de Ignacio de la Llave;
3. Ley 848 de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave;
4. Ley 581 para la Tutela dc Datos Personales en el Estado de Veracruz;
5. Reglamento de Transparencia, Acceso a la Información y Protección de Datos Personales;
6. Norma ISO/IEC 27001:2013 Tecnología de la información-Técnicas de seguridad-Sistemas de gestión de seguridad de la información-Requerimientos.

Se expiden en la ciudad de Xalapa, Ver., a los 26 días del mes de marzo del año dos mil catorce.

Mtra. Elsa Ortega Rodríguez
Directora General de Tecnología de Información