Universidad Veracruzana

Legislación Universitaria

Reglamento para la Seguridad de la Información

Índice

Presentación

Actualmente la información juega un papel preponderante para promover el desarrollo, incrementar el nivel de competitividad y alcanzar el éxito de una institución, siendo ésta un elemento clave para el cumplimiento de los objetivos estratégicos. La Universidad Veracruzana no es la excepción, genera y recibe información en su quehacer cotidiano a través de sus cuerpos académicos, investigaciones, estrategias, procesos, productos y servicios, además de la información relativa a su personal y alumnos.

En este contexto, es de relevancia mencionar que la información forma parte importante de los activos de información de la institución, al igual que las personas, los procesos, el *software*, *hardware*, medios de soporte de información, espacios físicos, red de telecomunicaciones, entre otros; los cuales deben protegerse por el valor que tienen para la Universidad, y son necesarios para mantener en operación los procesos institucionales.

Nuestra máxima casa de estudios, mantiene la apertura para adaptarse a los procesos de cambio del entorno y atender las demandas de la comunidad universitaria y la sociedad en general, entre los cambios más perceptibles es la rápida evolución, convergencia y uso intensivo de las tecnologías de información que ha posibilitado el acceso, de forma casi inmediata a la información generada por la Institución. En ese sentido, su principal compromiso es establecer la normatividad necesaria que regule, tanto el tratamiento adecuado como su salvaguarda; razón que dio origen al presente Reglamento de la Seguridad de la Información y que tiene como fundamento jurídico la Ley 581 para la Tutela de los Datos Personales para el Estado de Veracruz de Ignacio de la Llave y del Reglamento de Transparencia, Acceso a la Información y Protección de Datos Personales de la Universidad Veracruzana.

El Reglamento de la Seguridad de la Información de la Universidad Veracruzana tiene como objetivo principal, establecer el marco normativo para el uso de los activos de información, al mismo tiempo persigue los propósitos siguientes:

- Sensibilizar a los integrantes de la comunidad universitaria y usuarios externos en el cuidado, protección y responsabilidades asociadas al tratamiento de la información que no es pública;
- Mantener la confidencialidad, disponibilidad e integridad de la información personal e institucional; y
- Dar cumplimiento a las disposiciones legales en la materia.

Título I Disposiciones generales

Capítulo I
Disposiciones generales

Artículo 1. El presente Reglamento para la Seguridad de la Información de la Universidad Veracruzana es de observancia general y obligatoria para los integrantes de la comunidad universitaria, así como los usuarios externos que hagan uso de los activos de información de la misma. Regula las medidas de control para mantener la confidencialidad, integridad y disponibilidad de la información institucional.

Artículo 2. La Universidad Veracruzana establece acciones de manera continua para proteger los activos de información frente a riesgos y amenazas, con el fin de mantener la confidencialidad, integridad y disponibilidad de la información, contribuyendo a la continuidad de los procesos institucionales en apego a la legislación universitaria y normatividad en la materia.

Artículo 3. La información generada durante la jornada de trabajo de autoridades, funcionarios, personal académico, de confianza, personal administrativo, técnico y manual de la Universidad Veracruzana, así como trabajadores que se contraten para la realización de una obra o investigación determinada por la misma, será propiedad de la Universidad.

En la explotación del resultado deberá darse al trabajador que lo obtuvo, el crédito correspondiente; en caso de duda, se estará a lo dispuesto en la Ley Federal de Derechos de Autor.

Artículo 4. El usuario que realice tratamiento de la información, haga uso de los servicios de tecnologías de información, así como de la infraestructura tecnológica de la Universidad Veracruzana, acepta las medidas de control para salvaguardar la información establecidas en el presente Reglamento.

Artículo 5. Si surge la necesidad de intervenir un medio de soporte de información de la Universidad Veracruzana, asignado a un integrante de la comunidad universitaria durante el curso de alguna investigación de carácter judicial o administrativo por el uso inapropiado de los activos de información, la Institución deberá cumplir lo establecido en la Ley en la materia.

Artículo 6. Para efectos de este Reglamento, se considera:

I. **Confidencialidad.** Característica consistente en que la información es accesible únicamente por una persona, entidad o proceso autorizado;
II. **Cuenta institucional.** Identificador único de usuario que le permite acceder a los servicios de red y sistemas de información institucional;

III. **Disponibilidad.** Característica consistente en que la información se encuentra accesible y disponible cuando lo requiera una entidad, proceso o persona autorizada;
IV. **Integridad.** Característica consistente en el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso;
V. **Nombre de dominio.** Nombre fácil de recordar asociado a una o varias direcciones IP (Internet Protocol) de un equipo o servicio;
VI. **Usuarios.** Persona física o moral, interna o externa a la Universidad Veracruzana que utiliza los activos de información de la Institución.

Artículo 7. Cuando por exigencias de construcción gramatical, de enumeración, de orden, o por otra circunstancia cualquiera, el texto del Reglamento use o dé preferencia al género masculino, o haga acepción de sexo que pueda resultar susceptible de interpretarse en sentido restrictivo contra la mujer, éste deberá interpretarse en sentido igualitario para hombres y mujeres.

Capítulo II
De los activos de información

Artículo 8. Un activo de información es un elemento tangible o intangible que contiene o utiliza información de valor para la Institución y que es necesario para mantener la continuidad de sus procesos.

Artículo 9. Los activos de información se encuentran integrados de la manera siguiente:
I. **Información.** Conjunto de datos relacionados, almacenados, procesados, transmitidos, difundidos en la Institución mediante señales visuales, acústicas, ópticas o electromagnéticas;
II. **Proceso institucional.** Conjunto de actividades interrelacionadas necesarias para lograr los objetivos de la Institución, éstos implican y dependen de la información;
III. **Servicio.** Conjunto de actividades que buscan responder a las necesidades del usuario, incluye los servicios internos y externos que brinda la Universidad;
IV. **Área restringida.** Espacio físico donde se aloja información, *software*, *hardware*, medios de soporte o equipamiento auxiliar;
V. ***Software*.** Conjunto de programas, documentos, procesamientos y rutinas asociadas con la operación de un sistema de computadoras, es decir, la parte intangible o lógica;
VI. ***Hardware*.** Equipo tecnológico utilizado para gestionar la información y las comunicaciones;
VII. **Sitio web.** Conjunto de páginas y archivos electrónicos mediante los cuales se publica información institucional;

VIII. **Equipamiento auxiliar.** Equipo de soporte a los activos de información, entre los que se encuentran los equipos de destrucción de documentación, aires acondicionados, extintores, entre otros;
IX. **Red de telecomunicaciones.** Conjunto de elementos que permiten el intercambio de información electrónica entre dispositivos y computadoras, tales como cableado, equipos, protocolos y servicios.
X. **Medio de soporte.** Bien que permite el almacenamiento de información; y
XI. **Bien intangible.** Patentes, licencias de *software*, imagen y reputación que pertenecen a la Institución.

Capítulo III
De la seguridad de la información

Artículo 10. La seguridad de la información es el conjunto de medidas de control establecidas en la Universidad Veracruzana para mantener la confidencialidad, integridad y disponibilidad de la información, identificando, valorando y gestionando los riesgos en función del impacto que representan para la misma;

Artículo 11. La seguridad de la información se clasifica en:
I. **Seguridad física.** Es la condición que se alcanza aplicando las medidas de control para proteger los espacios físicos en los que se encuentran los activos de información; y
II. **Seguridad lógica.** Es la condición que se logra mediante el establecimiento de medidas de control para el acceso a la información digital y electrónica, así como los recursos de procesamiento de datos a los usuarios, sistemas informáticos, entidades y aplicaciones autorizadas.

Artículo 12. La medidas de control establecidas para alcanzar la seguridad física y lógica se clasifican de la manera siguiente:
I. **Normativas.** Siendo estas el Reglamento para la Seguridad de la Información, políticas, procedimientos, planes, especificaciones, manuales, instructivos operativos y buenas prácticas de seguridad de la información; y
II. **Técnicas.** Son las establecidas con el apoyo de herramientas y elementos para reducir la exposición de los activos de información ante situaciones de riesgo, tales como puertas, muros, tarjetas electrónicas, cuentas de acceso, *software*, entre otras.

Capítulo IV
De los objetivos de la seguridad de la información

Artículo 13. Los objetivos de la seguridad de la información son salvaguardar la información institucional así como todos los activos de información implicados en su tratamiento frente a riesgos y amenazas, estableciendo medidas de control para mantener la confidencialidad, integridad y disponibilidad de la misma. Los titulares de las entidades académicas y dependencias deberán observar lo siguiente:

I. Administrar los activos de información;
II. Gestionar los riesgos asociados a los activos de información de los procesos críticos institucionales, en función del impacto en la continuidad de las operaciones;
III. Establecer las medidas normativas y técnicas;
IV. Establecer indicadores para evaluar las medidas de control y proponer mejoras a partir de los resultados de la evaluación; y
V. Fomentar una cultura de seguridad de la información.

Título II De la distribución de competencias en materia de seguridad de la información

Capítulo único
De la distribución de competencias en materia de seguridad de la información

Artículo 14. La competencia en la Universidad Veracruzana para conocer en materia de seguridad de la información quedará distribuida conforme a lo siguiente:

I. **El Comité para la Seguridad Informática de los Datos Personales:** analizar y establecer las medidas de seguridad de los datos personales contenidos en las bases de datos de los Sistemas Informáticos, con base en la Ley 581 para la Tutela de los Datos Personales para el Estado de Veracruz de Ignacio de la Llave y en los Lineamientos que al efecto expida el IVAI, su integración y atribuciones se encuentran establecidas en el Reglamento de Transparencia, Acceso a la Información y Protección de Datos Personales;
II. **El Comité Estratégico de Tecnologías de la Información de la Universidad Veracruzana:** aprobar los riesgos residuales derivados de la evaluación y tratamiento de riesgos relativos a las tecnologías de la información de la Universidad Veracruzana, su integración y atribuciones se encuentran establecidas en el Acuerdo del Rector emitido con fecha 22 de septiembre de 2016;
III. **El Consejo Consultivo del Sistema Universitario de Gestión Integral del Riesgo de la Universidad Veracruzana (SUGIR-UV):** realizar análisis de riesgo y acciones de prevención y respuesta ante fenómenos naturales, antro-

pogénicos que pongan en riesgo, bienes muebles e inmuebles de la Universidad en el cual se alojen activos de información, su integración y atribuciones se encuentran establecidas en el Acuerdo del Rector emitido con fecha 16 de mayo de 2013;

IV. **El Director General de Tecnología de Información:** implementar las medidas de control de la seguridad para salvaguardar la información durante el diseño, desarrollo e implementación de proyectos de Tecnologías de Información institucionales requeridos para el funcionamiento y operatividad de la Universidad Veracruzana en el ámbito de su competencia, con fundamento en lo establecido en los artículos 32 la Ley 581 para la Tutela de Datos Personales en el Estado de Veracruz;

V. **Los titulares de las entidades académicas y dependencias:** implementar las medidas de control institucionales para la seguridad, así como aquellas de control interno necesarias para salvaguardar la integridad, disponibilidad y confidencialidad de información que se encuentra bajo su responsabilidad;

VI. **El Director de Control de Bienes Muebles e Inmuebles:** establecer las medidas de control técnicas para la destrucción controlada de medios utilizados para el almacenamiento o respaldo de información digital o electrónica, previo al proceso de baja del bien para evitar su acceso y su recuperación posterior.

Título III
De la seguridad física y lógica de los activos de información

Artículo 15. La Universidad Veracruzana establece medidas de control de seguridad física y lógica para salvaguardar la integridad, confidencialidad y disponibilidad de la información.

Las medidas de control de seguridad física permiten proteger los espacios físicos en los que se encuentran los activos de información y las medidas de control de seguridad lógica permiten verificar el acceso a la información digital y electrónica.

Capítulo I
De la seguridad física de los activos de información

Artículo 16. Las medidas de control para la seguridad física con que cuenta la Universidad son:

I. Acceso a las áreas restringidas; y

II. Protección de las tecnologías de información.

Sección primera

Del acceso a las áreas restringidas

Artículo 17. Un área restringida es el espacio físico en las instalaciones de la Universidad Veracruzana que salvaguarda información, *software*, *hardware*, medios de soporte o equipamiento auxiliar y al cual tiene acceso sólo personal autorizado por el titular de la entidad académica o dependencia.

Artículo 18. El titular de la entidad académica o dependencia donde se ubica el área restringida deberá cumplir y hacer cumplir las medidas de control para la seguridad física institucional, así como establecer las medidas internas para salvaguardar la confidencialidad, integridad y disponibilidad de información que se encuentra bajo su responsabilidad;

Artículo 19. El acceso al área restringida se permitirá, previa autorización del titular de la entidad académica o dependencia, en los términos establecidos en el Procedimiento para el Control de Acceso a Áreas Restringidas publicado en el portal institucional.

El incumplimiento de lo anterior será considerado una falta y será sancionado de acuerdo con lo establecido en la legislación universitaria, si al investigar las faltas de carácter universitario se advierte la comisión de un delito, deberá hacerse la denuncia a las autoridades competentes, sin perjuicio de que se imponga la sanción prevista por la reglamentación respectiva.

Artículo 20. El integrante de la comunidad universitaria que detecte personas ajenas sin autorización en un área restringida, deberá informar al titular de la entidad académica o dependencia, al administrador o al vigilante en turno.

Artículo 21. Queda prohibida la toma de fotografías o grabación de videos y audios, dentro del área restringida, salvo que previamente se haya obtenido la autorización por escrito del titular de la entidad académica o dependencia.

Artículo 22. El titular de la entidad académica o dependencia donde se ubica el área restringida, será responsable de establecer:

I. Letreros de señalización del área restringida;
II. Directorio de personal pre-autorizado;
III. Equipamiento auxiliar en óptimas condiciones; y
IV. Registro de incidentes.

Sección segunda
De la protección de las Tecnologías de Información

Artículo 23. La protección de las Tecnologías de Información utilizadas para el almacenamiento, recuperación, protección, procesamiento, difusión y transmisión de la información que se encuentran a disposición de la comunidad universitaria, es necesaria debido a que brindan soporte a los procesos que realizan las entidades académicas y dependencias, entre las que se encuentran los sistemas informáticos, aplicaciones, servicios digitales, servidores, infraestructura y servicios de telecomunicaciones, equipo de cómputo, sistemas de almacenamiento, dispositivos periféricos y móviles, entre otros.

Artículo 24. Los titulares de las entidades académicas y dependencias deberán vigilar que los recursos de tecnologías de información se encuentren en condiciones apropiadas de operación, realizar el mantenimiento correspondiente y vigilar que se destinen al cumplimiento de las funciones para los que fueron adquiridos o desarrollados, observando lo siguiente:

I. La colocación, reubicación, configuración, instalación o desinstalación de equipo activo de telecomunicación, entendiéndose éste como cualquier componente de red que genera o modifica las señales mediante las cuales se transmite la información, se deberá solicitar a la Dirección General de Tecnología de Información mediante la mesa de ayuda;
II. La adquisición de equipo activo de telecomunicación solo será con equipos que cumplan con las especificaciones autorizadas por la Dirección General de Tecnología de Información;
III. Los contactos de energía eléctrica regulada deberán utilizarse únicamente para conectar recursos de tecnologías de información, en caso de no contar con ésta, el titular de la entidad académica o dependencia deberá gestionar la instalación de un sistema de regulación de la misma;
IV. En caso de que un recurso de tecnologías de información tenga vigente la póliza de seguro, deberá enviarse al proveedor correspondiente para hacerla válida, previo respaldo y borrado de la información;
V. Cuando algún activo de la infraestructura de telecomunicaciones institucional presente alguna falla, deberá reportarse en la mesa de ayuda para proceder a realizar el diagnóstico correspondiente; y
VI. El titular de la entidad académica o dependencia deberá designar a un encargado con los conocimientos técnicos necesarios, para revisar y dar soporte a los recursos de tecnologías de información, previo reporte en la mesa de ayuda.

Artículo 25. El responsable técnico que atiende los servicios de videoconferencias que ofrece la Universidad Veracruzana, a través de las salas ubicadas en las Unidades de Servicios Bibliotecarios y de Información (USBI), sólo realizará la grabación

de eventos de videoconferencia a solicitud expresa del usuario y no resguardará respaldo de dicha grabación, entendiéndose como un evento de videoconferencia a la actividad consistente en la atención de usuarios en recintos habilitados con capacidad de transmisión de videoconferencias.

Artículo 26. Los usuarios de las tecnologías de información estarán obligados a cumplir las medidas de control para la seguridad establecidas en este Reglamento, el incumplimiento de lo anterior será considerado una falta y será sancionado de acuerdo con lo establecido en la legislación universitaria.

Capítulo II
De la seguridad lógica de los activos de información

Artículo 27. La seguridad lógica es la condición que se logra mediante el establecimiento de medidas de control para el acceso a la información digital y electrónica, así como a los recursos de procesamiento de datos.

Artículo 28. Las medidas de control para la seguridad lógica son:

I. El control de acceso lógico, de la cuenta y correo electrónico institucional;
II. La administración del *software*;
III. De la red de telecomunicaciones y servidores; y
IV. Detección y contención de código malicioso.

Capítulo III
Del control de acceso lógico, de la cuenta y correo electrónico institucional

Sección primera
Del control de acceso

Artículo 29. El control de acceso lógico se refiere a las medidas de control que permiten la autenticación de los usuarios autorizados a los servicios de tecnologías de información de acuerdo con las funciones que desempeñan. Se entiende por autenticación al procedimiento informático que permite verificar que el usuario de un servicio es quien dice ser.

Sección segunda
De la cuenta institucional

Artículo 30. Los usuarios que requieran acceder a los servicios de tecnologías de información, deberán contar con una cuenta institucional personal e intransferible, conformada por un nombre de usuario y contraseña, la cual podrá solicitar el titular de la entidad académica o dependencia, atendiendo al Procedimiento de Apertura de Cuenta Institucional publicado en el portal institucional.

Se entiende por contraseña al conjunto de caracteres que permiten el acceso de un usuario a un servicio de tecnología de información.

Artículo 31. Las medidas de control para proteger la cuenta institucional que se deberán observar son:

I. El usuario deberá resguardar y no compartir su cuenta institucional utilizada para el desempeño de sus funciones, ya que será responsable de las acciones que se realicen en su nombre;
II. El usuario que sospeche de robo o suplantación de su cuenta institucional deberá solicitar su cambio de contraseña mediante el Procedimiento de Actualización de Cuenta publicado en el portal institucional;
III. Cuando el personal deje de laborar en la Institución, el titular de la entidad académica o dependencia deberá solicitar la baja de la cuenta institucional asignada conforme al Procedimiento de Baja de Cuenta Institucional publicado en el portal institucional;
IV. Cuando el personal sea transferido a otra entidad académica o dependencia de adscripción, el titular de la misma donde estaba adscrito, deberá solicitar la baja de los permisos de acceso a los servicios;
V. El usuario que requiera acceder a los servicios de tecnologías de información vía remota, deberá realizarlo a través de una Red Privada Virtual (VPN) que deberá solicitar a través del Procedimiento de Servicios de Red publicado en el portal institucional; y
VI. Cuando un usuario externo deje de prestar sus servicios a la Institución y que por la naturaleza de sus actividades haya requerido el acceso a los servicios de tecnologías de información, el titular de la entidad académica o dependencia, deberá solicitar la revocación de los permisos de acceso a los servicios.

Sección tercera
Del correo electrónico institucional

Artículo 32. El correo electrónico institucional es una herramienta de trabajo para el intercambio de información entre distintos equipos informáticos interconectados, a través de una red de telecomunicaciones.

La Universidad Veracruzana pone a disposición del personal y alumnos una cuenta de correo electrónico institucional en apoyo a sus actividades.

Artículo 33. Las medidas de control para la protección del correo electrónico institucional que deberán observar los usuarios son:

I. Se prohibe el envío de cadenas de mensajes de correo, correos masivos no institucionales, de contenido comercial, de esparcimiento, con fines de lucro o para ofrecer servicios;
II. El usuario que reciba un mensaje de correo electrónico cuyo origen sea desconocido o de dudosa procedencia, deberá evitar abrirlo, borrarlo inmediatamente e informar a la Dirección General de Tecnología de Información y en su caso, a los responsables Regionales de Tecnología de Información correspondiente;
III. La Dirección General de Tecnología de Información, al detectar un excesivo flujo de información por mensajes y archivos podrá suspender temporalmente la cuenta de correo electrónico del usuario que origina dicho flujo para que el servicio de correo institucional no se vea afectado;
IV. El alumno que sea dado de baja definitiva perderá el derecho a su cuenta de correo institucional y tendrá 30 días hábiles para respaldar su información antes de que sea eliminada;
V. Ningún usuario deberá suplantar la identidad de otro usuario; y
VI. El incumplimiento de cualquier regulación vigente por la transmisión de información digital y electrónica por este medio será responsabilidad el usuario.

Capítulo IV

De la administración del *software*

Artículo 34. La administración del *software* propiedad de la Universidad Veracruzana es el proceso que involucra la planificación, organización, ejecución y control del mismo; el cual se pone a disposición de los integrantes de la comunidad universitaria.

Artículo 35. La administración del *software* con licencia de cobertura institucional es responsabilidad de la Dirección General de Tecnología de Información. Entendiéndose por *software* con licencia de cobertura institucional a los programas que cuentan con un licenciamiento de cobertura masiva, utilizados por los integrantes de la comunidad universitaria en el parque computacional de la Institución.

Artículo 36. El usuario únicamente deberá instalar en los equipos de cómputo y de red institucionales *software* que cuente con la licencia correspondiente y que se justifique para las actividades descritas en sus funciones.

La descarga, uso o distribución de software sin la licencia correspondiente será responsabilidad del usuario y se sancionará conforme a la legislación universitaria vigente y leyes aplicables.

Artículo 37. La administración de *software* con licencia adquirido por una entidad académica o dependencia será responsabilidad del titular de la misma.

Artículo 38. El titular de la entidad académica o dependencia que requiera desarrollar un sistema informático, portal o aplicaciones de cobertura institucional deberá enviar a la Dirección General de Tecnología de Información la cédula de Proyecto para que en conjunto con el Comité Estratégico de Tecnologías de Información sea analizado y en su caso autorizado, apegándose al Procedimiento de Gestión de Proyectos publicado en el portal institucional.

Artículo 39. En el caso de sistemas informáticos, portales o aplicaciones de uso institucional en operación, el titular de la entidad académica o dependencia deberá realizar su formalización mediante la cédula de registro ante la Dirección General de Tecnología de Información para ser turnado al Comité Estratégico de Tecnologías de Información para su autorización.

Capítulo V

De la red de telecomunicaciones y servidores

Artículo 40. La red de telecomunicaciones de la Universidad Veracruzana es el conjunto de elementos que permiten el intercambio de información electrónica entre dispositivos y computadoras, tales como cableado, equipos, protocolos y servicios, con la finalidad de apoyar a las actividades de los integrantes de la comunidad universitaria; se clasifica en:

I. Red alámbrica. Conjunto de dispositivos conectados entre sí por un medio físico.
II. Red inalámbrica. Conjunto de dispositivos conectados entre sí por medio de señales electromagnéticas.

Artículo 41. La configuración e instalación de equipos de red de área local y permisos para realizar conexiones remotas a redes internas o externas en la Universidad deberán ser autorizadas por la Dirección General de Tecnología de Información.

Artículo 42. La configuración de los servidores y equipo de telecomunicación alojados en sitios de telecomunicaciones institucionales sólo la realizará personal autorizado por la Dirección General de Tecnología de Información.

Artículo 43. El equipo de cómputo o dispositivo que presente un comportamiento que comprometa la seguridad de la información o la disponibilidad de la red de telecomunicaciones será desconectado por la Dirección General de Tecnología de Información, notificando por escrito al titular de la entidad académica o dependencia y realizando una evaluación del caso que permita determinar la responsabilidad de acuerdo con la legislación universitaria y leyes de la materia aplicables.

Artículo 44. El usuario que tenga asignado un dispositivo móvil institucional o personal y que trate en el mismo información de la Universidad, deberá establecer las medidas de control de seguridad siguientes:

I. Configurar los servicios de *bluetooth* y *wifi* con contraseña;
II. Activar la opción de contraseña de arranque o bloqueo;
III. Activar la opción de apagado o bloqueo automático después de un determinado tiempo que no esté en uso;
IV. Validar la autenticidad de las aplicaciones que instale;
V. Realizar copias de seguridad de la información contenida en el dispositivo; y
VI. Activar la opción de monitoreo y rastreo de equipo para recuperar o borrar la información de forma remota en caso de pérdida.

Artículo 45. La Dirección General de Tecnología de Información se reserva el derecho de bloquear el acceso a cualquier usuario que atente contra el uso responsable, desempeño y la calidad de las tecnologías de información así como a los activos de información.

Artículo 46. El alojamiento de cualquier nombre de dominio distinto al institucional en los servidores de la Universidad, deberá ser autorizado por la Dirección General de Tecnología de Información.

Artículo 47. El usuario que requiera de la contratación de un nombre de dominio o servicio de hospedaje distinto al institucional para el desempeño de sus actividades de divulgación de información institucional en la internet, deberá contar con la autorización del Comité Estratégico de Tecnologías de Información.

Artículo 48. El diseño, administración y contenido de los portales web será responsabilidad de cada titular de la entidad académica o dependencia, de acuerdo con sus requerimientos de difusión de información y apegándose al Estándar de Diseño del Portal Web Institucional publicado en el portal institucional.

Artículo 49. Ningún usuario se encuentra autorizado para alojar información reservada o confidencial en la nube, sin previa autorización del Comité Estratégico de Tecnologías de Información. Entendiéndose por nube a los servicios de almacenamiento o de procesamiento de información a través de Internet contratados con proveedores externos.

Artículo 50. El usuario autorizado para alojar servicios de tecnología de información en la nube deberá asegurarse que se establezcan las medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información.

Capítulo VI
Detección y contención de código malicioso

Artículo 51. El usuario que tenga asignado un recurso de tecnología de información y patrimonio de la Universidad deberá hacer uso de *software* con licencia para la protección contra código malicioso.

El código malicioso es un programa informático cuyo objetivo es ocasionar daño a activos de información tales como información, servicios, sitios web, red de telecomunicaciones, entre otros.

Artículo 52. El usuario que reciba información a través de cualquier medio digital susceptible de ser leída, descargada y almacenada en un recurso de tecnología de información institucional, deberá verificar que no cuente con código malicioso mediante la ejecución de un *software* antivirus actualizado.

Artículo 53. El usuario que cuente con *software* antivirus institucional deberá mantenerlo y respetar la configuración de seguridad del recurso de tecnología de información institucional asignado para detectar o prevenir la propagación de código malicioso.

Título IV De las responsabilidades y las sanciones

Capítulo I
De las responsabilidades

Artículo 54. Los integrantes de la comunidad universitaria serán responsables de cualquier daño a los activos de información por actos u omisiones que les sean imputables o por incumplimiento o inobservancia de obligaciones derivadas de este Reglamento y las leyes en la materia.

Artículo 55. Las autoridades, funcionarios, personal académico, de confianza, administrativo técnico y manual que en el ejercicio de sus funciones realice tratamiento de información que no sea pública, deberá:

I. Actuar bajo los más estrictos principios de confidencialidad conforme a lo establecido en el Reglamento de Transparencia, Acceso a la Información y Protección de Datos Personales de la Universidad Veracruzana;

II. Suscribir la responsiva y compromiso de confidencialidad; y
III. Salvaguardar la información, propiedad de la Universidad Veracruzana.

Artículo 56. Los integrantes de la comunidad universitaria en el desarrollo de sus actividades, deberán observar lo siguiente:
I. Cumplir y hacer cumplir este Reglamento;
II. Promover entre los integrantes de la comunidad universitaria conocimientos y conciencia de la importancia de las medidas de control de la seguridad de la información;
III. Adoptar las medidas necesarias y adecuadas para el uso responsable de los activos de información utilizados en el ejercicio de sus funciones;
IV. Participar en la capacitación y actualización en materia de seguridad de la información, así como cualquier otra forma de enseñanza y entrenamiento que se considere pertinente; y
V. Aplicar en su ámbito de competencia, las políticas y los acuerdos emitidos por los Órganos Colegiados establecidos en este Reglamento.

Capítulo II
De las sanciones

Artículo 57. El usuario que transgreda las medidas de control para la seguridad de la información física o lógica establecidas en el presente Reglamento y en los procedimientos públicados en el portal institucional se hará acreedor a la sanción correspondiente de acuerdo, con la legislación universitaria vigente y las leyes aplicables.

Artículo 58. La Universidad se reserva el derecho a ejercer las acciones legales para la protección y defensa de sus legítimos intereses en aquellos supuestos de hecho no contemplados en el presente Reglamento, que pudiesen tener cabida al Código Penal o cualquier otra legislación vigente.

Artículo 59. Constituyen causales de sanción que atentan en contra de la seguridad de la información las siguientes:
I. Realizar actividades de intercepción o revelación de comunicación electrónica;
II. Realizar análisis de vulnerabilidades no autorizado que atente contra la seguridad de los activos de información, así como el uso de aplicaciones no autorizadas que operen en la red de telecomunicación universitaria;
III. Comercializar información propiedad de la Institución; y
IV. Divulgar información reservada o confidencial violando los términos establecidos en el Reglamento de Transparencia, Acceso a la Información y Protección de Datos Personales.

Artículo 60. El desconocimiento del presente Reglamento por parte del usuario no lo exime de las responsabilidades y sanciones a que se haga acreedor en términos de la Legislación Universitaria vigente y demás disposiciones que en materia de seguridad de la información se señalen para tal efecto.

Transitorios

Primero. El presente Reglamento entrará en vigor al día siguiente de su aprobación por el H. Consejo Universitario General.

Segundo. Se abroga la Política de Seguridad de la Información aprobada el 28 de septiembre de 2015 por el Comité para la Seguridad Informática de los Datos Personales.

Tercero. Se establece un plazo de sesenta días hábiles para que la Dirección General de Tecnología de Información en Coordinación con la Unidad de Organización y Métodos actualice los formatos y procedimientos necesarios para la implementación del presente Reglamento.

Cuarto. Publíquese, difúndase y cúmplase.

Aprobado en sesión del H. Consejo Universitario General celebrada el día 14 de diciembre de 2016.

Dirección de Normatividad.