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 la institución, al igual que las personas, los procesos, el *software*, el *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 por ser necesarios para mantener en operación los procesos institucionales.

Por otra parte, 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 de la Universidad Veracruzana y que tiene como fundamento jurídico la Ley General de Archivo, la Ley Núm. 316 de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Veracruz de Ignacio de la llave, el Reglamento de Responsabilidades Administrativas y el Reglamento de Transparencia, Acceso a la Información y Protección de Datos Personales de la Universidad Veracruzana.

Adicionalmente, debido a que la Universidad Veracruzana es una institución que administra recursos públicos, es importante mantener un ambiente de control interno en la gestión universitaria como aliado para la transparencia y la rendición de cuentas, otorgando un grado de seguridad razonable en cuanto a la consecución de los objetivos y metas estratégicas establecidas, cuidando la eficacia y la eficiencia de las operaciones, así como la disponibilidad de la información financiera y no financiera confiable, oportuna y de calidad, esto en cumplimento de leyes, regulaciones y normas aplicables. La implementación del Sistema de Control Interno Institucional se encuentra coordinado por el Comité de Control y Desempeño Institucional (COCODI) quien promueve el establecimiento de la normatividad y medidas administrativas necesarias que permiten gestionar eficientemente los riesgos asociados al control interno y a los sistemas de información institucionales, ya sean manuales o automatizados.

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: mantener la confidencialidad, disponibilidad e integridad de la información personal e institucional; 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, así como dar cumplimiento a las disposiciones legales y 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 para 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, con el fin de mantener la confidencialidad, integridad y disponibilidad de la información, que contribuyen 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 del personal de la Universidad Veracruzana, así como trabajadores que se contraten para la realización de una obra o investigación determinada, será propiedad de la Institución.

En la explotación de este resultado, debe darse al trabajador que lo obtuvo, el crédito correspondiente; en caso de duda, se estará a lo dispuesto en la Ley Federal del Derecho 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 establecida 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 debe cumplir lo establecido en la Ley en la materia.

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

I. **Confidencialidad.** Consiste en que la información es accesible únicamente por una persona, entidad o proceso autorizado, incluye el registro, custodia y cuidado de la documentación e información que, por razón de su empleo, cargo o comisión, tenga bajo su responsabilidad;
II. **Cuenta institucional.** Identificador único de usuario que le permite acceder a los servicios de red y sistemas de información institucional;
III. **Disponibilidad.** Consiste en que la información se encuentra accesible y disponible cuando lo requiera una entidad, proceso o persona autorizada;
IV. **Integridad.** Consiste en el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso;
V. **Nombre de dominio.** Nombre asociado a una o varias direcciones IP (Internet Protocol, por sus siglas en inglés; protocolo de internet, en español), de un equipo o servicio; y
VI. **Usuario.** 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 presente 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 debe 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 o que es necesario para mantener la continuidad de sus procesos.

Artículo 9. Los activos de información se encuentran clasificados 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;
IV. **Área restringida.** Espacio físico donde se alojan otros activos de información y específicamente información institucional clasificada como reservada o confidencial;
V. ***Software*.** Programas, documentos, procesamientos y rutinas asociadas con la operación de un sistema de computadoras;
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 tales como cableado, equipos, protocolos y servicios, que permiten el intercambio de información digital entre dispositivos electrónicos; y
X. **Medio de soporte.** Bien mueble que permite el almacenamiento de información.

Capítulo III
De la seguridad de la información

Artículo 10. La seguridad de la información es el conjunto de medidas de control establecido 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 institución, para impedir o evitar su uso, divulgación, sustracción, destrucción, ocultamiento o inutilización indebidos.

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 el entorno físico en el 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 intangible almacenada en medio digital o

electrónico, así como los recursos de procesamiento de datos a los usuarios, sistemas informáticos, entidades y aplicaciones autorizadas.

Artículo 12. Las medidas de control establecidas para alcanzar la seguridad física y lógica se clasifican de la manera siguiente:

I. **Normativas.** Conjunto de normas contenidas en el Reglamento para la Seguridad de la Información y el Reglamento de Transparencia, Acceso a la Información y Protección de Datos Personales, Reglamento de Responsabilidades Administrativas y leyes aplicables en la materia;
II. **Administrativas.** Conjunto de políticas y procedimientos para la gestión, buenas prácticas para el soporte y revisión de la seguridad de la información a nivel institucional; y
III. **Técnicas.** Conjunto de acciones y mecanismos que se valen de la tecnología para reducir la exposición de los activos de información ante situaciones de riesgo en el entorno digital.

Capítulo IV
Del objetivo de la seguridad de la información

Artículo 13. El objetivo de la seguridad de la información es 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.

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 de Control y Desempeño Institucional:** es responsable de aprobar las estrategias y líneas de acción para contar en la Universidad Veracruzana con herramientas de información y comunicación con los más altos estándares en su infraestructura tecnológica y de seguridad para facilitar y respaldar el control interno, considerando que la información y la comunicación deben ser confiables, oportunas, seguras, accesibles, pertinentes y verificables, porque son vitales para la consecución de la metas y el cumplimiento de las normas que rigen la conducta institucional;
II. **El Comité Estratégico de Tecnologías de la Información:** es responsable de aprobar los riesgos residuales derivados de la evaluación y tratamiento de riesgos relativos a las tecnologías de la información de la Universidad Veracruzana;
III. **El Consejo Consultivo del Sistema Universitario de Gestión Integral del Riesgo:** es responsable de llevar a cabo el análisis de riesgo y acciones de prevención y respuesta ante fenómenos naturales, antropogénicos que pongan en riesgo, bienes muebles e inmuebles de la Universidad en el cual se alojen activos de información;
IV. **La Dirección General de Tecnología de Información:** es responsable de implementar las medidas de control 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;

V. **El titular de la entidad académica o dependencia:** es responsable de registrar, integrar, custodiar y cuidar los activos de información que, por razón de su empleo, cargo o comisión, tenga bajo su responsabilidad, e impedir o evitar su uso, divulgación, sustracción, destrucción, ocultamiento o inutilización indebidos, así como identificar, mitigar, eliminar, transferir los riesgos asociados a los mismos. Además de contribuir al fortalecimiento de una cultura de seguridad de la información institucional;

VI. **La Dirección de Control de Bienes Muebles e Inmuebles:** es responsable de 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; y

VII. **El Centro de Investigación en Documentación sobre la Universidad:** es responsable de vigilar el cumplimiento de las normas, políticas y medidas técnicas para la regulación de los procesos archivísticos durante el ciclo vital de los documentos de archivo, que se expidan para la clasificación, preservación y conservación de los documentos históricos.

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 que establece 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 activos de información 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 debe 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 es 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, debe 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, debe informar al titular de la entidad académica o dependencia, al administrador o al vigilante en turno.

Artículo 21. El titular de la entidad académica o dependencia donde se ubica el área restringida es responsable de aplicar las medidas de control establecidas en el Procedimiento de Acceso a Áreas Restringidas, publicado en el portal institucional, entre las que se encuentran las siguientes:

I. Señalética de área restringida;
II. Directorio de personal preautorizado;
III. Equipamiento auxiliar en óptimas condiciones;
IV. Registro de incidentes; y
V. Bitácora de acceso.

Artículo 22. Sólo se podrá tomar fotografías y grabar videos en un área restringida, si se cuenta con la autorización previa por escrito del titular de la entidad académica o dependencia donde se encuentre ubicada la misma.

Sección segunda
De la protección de las tecnologías de información

Artículo 23. Las tecnologías de información son todas aquellas utilizadas para el almacenamiento, recuperación, protección, procesamiento, difusión y transmisión de la información que se encuentran a disposición de la comunidad universitaria.

La protección de las tecnologías de información 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, infraestructura y servicios de telecomunicaciones, equipo de cómputo, sistemas de almacenamiento, dispositivos periféricos y móviles, entre otros.

Artículo 24. El titular de la entidad académica y dependencia debe vigilar que las tecnologías de información bajo su tramo de control se encuentren en condiciones apropiadas de operación, así como realizar el mantenimiento correspondiente y vigilar que se destinen al cumplimiento de las funciones para las que fueron adquiridos o desarrollados, observando lo siguiente:

I. La adquisición de equipo activo de telecomunicación, equipo de cómputo y periférico, deberá realizarse en apego a lo establecido en los Estándares Institucionales de Equipo de Cómputo y Periféricos vigentes emitidos por el Comité Estratégico de Tecnologías de la Información, publicados por la Dirección de Recursos Materiales en el portal institucional;
II. El titular debe designar a un encargado con los conocimientos técnicos necesarios, para revisar y dar soporte a los activos de tecnologías de información;
III. 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 debe solicitar por escrito a la Dirección General de Tecnología de Información;

IV. Los contactos de energía eléctrica regulada deben utilizarse únicamente para conectar activos de tecnologías de información; en caso de no contar con estos, el titular debe gestionar ante la Dirección de Proyectos, Construcciones y Mantenimiento, la instalación de un sistema de regulación de la misma;

V. En caso de que un activo de tecnologías de información presente un fallo o daño, y tenga vigente la póliza de mantenimiento o garantía, debe enviarla al proveedor correspondiente para hacerla válida, previo respaldo y borrado de la información, así como avisar a la Dirección de Recursos Materiales como entidad responsable de las adquisiciones; y

VI. Cuando algún activo de información presente alguna falla, éste no cuente con póliza de garantía y la entidad académica o dependencia no cuente con personal técnico, debe reportarse por escrito a la Dirección General de Tecnología de Información para proceder a realizar el diagnóstico correspondiente.

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, 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.

El responsable técnico no hará grabaciones de los eventos o videoconferencia realizados fuera de las Unidades de Servicios Bibliotecarios y de Información.

Artículo 26. El usuario de las tecnologías de información está obligado a cumplir las medidas de control para la seguridad establecidas en este Reglamento, el incumplimiento de lo anterior es considerado una falta y será sancionado de acuerdo con lo establecido en la legislación universitaria.

Artículo 27. Informar por escrito al inmediato superior y en su caso al superior jerárquico, la identificación de algún riesgo sobre la seguridad de los activos de información.

Capítulo II
De la seguridad lógica de los activos de información

Artículo 28. La seguridad lógica es la condición que se logra mediante el establecimiento de medidas de control para salvaguardar la información digital y electrónica, así como a los recursos de procesamiento de datos.

Artículo 29. Las medidas de control para la seguridad lógica son:

I. El control de acceso a los servicios de tecnología de la información mediante la cuenta institucional;

II. La administración del *software*;

III. De la red de telecomunicaciones y servidores;

IV. Detección y contención de código malicioso; y

V. De la ciberseguridad.

Capítulo III
Del control de acceso a los servicios de tecnologías de la información, mediante la cuenta institucional

Sección primera
Del control de acceso

Artículo 30. El control de acceso lógico se refiere a las medidas de seguridad que permiten la autenticación del usuario autorizado a los servicios de tecnologías de información, de acuerdo con las funciones que desempeña. Se entiende por autenticación el procedimiento informático que permite verificar que el usuario de un servicio es quien dice ser.

Sección segunda
De la cuenta institucional

Artículo 31. El usuario que requiera acceder a los servicios de tecnologías de información debe contar con una cuenta institucional personal e intransferible, conformada por un nombre de usuario y contraseña, la cual es solicitada por el titular de la entidad académica o dependencia, atendiendo al Procedimiento Gestión de Cuentas Institucionales publicado en el portal institucional.

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

Artículo 32. Las medidas de control que el usuario debe observar para proteger la cuenta institucional son las siguientes:

I. 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. Solicitar el cambio de contraseña, cuando la extravíe, sospeche del robo de su cuenta institucional o suplantación de identidad, mediante el Procedimiento de Actualización de Cuenta Institucional publicado en el portal web;
III. El titular de la entidad académica o dependencia debe solicitar la eliminación de una cuenta institucional, conforme al Procedimiento de Baja de Cuenta Institucional publicado en el portal institucional, cuando un usuario deje de laborar o prestar sus servicios a la Institución;
IV. Cuando el personal cambie de adscripción o se modifique su estatus laboral, el jefe inmediato, debe solicitar la actualización de la información conforme al Procedimiento Gestión de Cuentas Institucionales publicado en el portal institucional; y
V. El responsable de cada sistema de información que utilice la cuenta institucional como medio acceso al mismo, debe establecer los niveles de seguridad conforme al perfil del usuario.

Artículo 33. El usuario que haga uso de las tecnologías de información que proporciona la Universidad fuera de las instalaciones universitarias, debe apegarse a las medidas de control siguientes:

I. Solicitar el acceso a través de una Red Privada Virtual mediante el Procedimiento de Servicios de Red publicado en el portal institucional; y
II. Salvaguardar la información conforme a lo establecido en el presente reglamento y leyes aplicables en la materia.

Sección tercera
Del correo electrónico institucional

Artículo 34. 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 35. Las medidas de control que el usuario debe cumplir para la protección del correo electrónico institucional son las siguientes:

I. Se prohíbe suplantar la identidad de otro usuario, ceder y divulgar a terceros listas de correo electrónico institucional, así como el envío de mensajes de correo en cadena, correos masivos no institucionales, de contenido comercial, de esparcimiento, con fines de lucro o para ofrecer servicios;
II. Al recibir un mensaje de correo electrónico cuyo origen sea desconocido o de dudosa procedencia, debe reportarlo al Centro de Servicios sin abrirlo y debe eliminarlo;
III. La información emitida o recibida por correo electrónico institucional debe preservar la conducta ética y profesional que el usuario debe mantener como miembro de la Institución; y
IV. El incumplimiento de cualquier regulación vigente por la transmisión de información digital y electrónica por este medio, es responsabilidad el usuario.

Artículo 36. El alumno que sea dado de baja definitiva pierde el derecho a su cuenta de correo institucional y tiene treinta días naturales para respaldar su información antes de que sea eliminada.

Artículo 37. Cuando una persona concluya su relación laboral con la Universidad, su cuenta institucional es inhabilitada 48 horas después de la petición realizada a la Dirección General de Tecnología de Información por el titular de la entidad académica o dependencia donde se encontraba adscrito o la Dirección General de Recursos Humanos.

Artículo 38. La información almacenada en el buzón de correo electrónico institucional solo podrá ser proporcionada cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente.

Artículo 39. Al detectar un excesivo flujo de información por mensajes y archivos en la cuenta de correo electrónico del usuario, la Dirección General de Tecnología de Información suspenderá temporalmente dicha cuenta para que el servicio de correo institucional no se vea afectado, informando al titular de la entidad académica o dependencia donde se encuentre adscrito el usuario.

Capítulo IV
De la administración del *software*

Artículo 40. La administración del *software*, propiedad de la Universidad Veracruzana, es el proceso que involucra la planificación, organización, ejecución y control del mismo a disposición de los integrantes de la comunidad universitaria.

Artículo 41. 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 42. El usuario únicamente debe 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 y leyes aplicables.

Artículo 43. La administración y resguardo del *software* con licencia es responsabilidad del titular de la entidad académica o dependencia.

Artículo 44. El titular de la entidad académica o dependencia que requiera desarrollar un sistema informático, portal o aplicación, debe apegarse al Procedimiento de Gestión de Proyectos publicado en el portal institucional.

Artículo 45. En el caso de sistemas informáticos, portales o aplicaciones de uso institucional en operación, el titular de la entidad académica o dependencia debe 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 46. La red de telecomunicaciones de la Universidad Veracruzana es el conjunto de elementos que permiten el intercambio de información digital 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; y
II. Red inalámbrica. Conjunto de dispositivos conectados entre sí por medio de señales electromagnéticas.

Artículo 47. La configuración e instalación de equipos de red y los permisos para realizar conexiones a redes internas o externas u otorgar servicios en la Universidad debe ser autorizada por la Dirección General de Tecnología de Información.

Artículo 48. La configuración de los servidores y equipo de telecomunicación alojados en sitios de telecomunicaciones institucionales y en áreas de acceso restringido, sólo la debe realizar el personal autorizado por la Dirección General de Tecnología de Información.

Artículo 49. El equipo de cómputo o dispositivo que presente un comportamiento que comprometa la disponibilidad de la red de telecomunicaciones o el desempeño de los servicios tecnológicos, 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 las leyes de la materia aplicables.

Artículo 50. El usuario que tenga asignado un dispositivo institucional o personal y que trate en el mismo información de la Universidad, debe establecer las medidas de control de seguridad siguientes:

I. Configurar los servicios de bluetooth y wifi con contraseña, en caso que aplique;
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, en caso que aplique.

Artículo 51. 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 52. El alojamiento de cualquier nombre de dominio distinto al institucional en los servidores de la Universidad, debe ser autorizado por la Dirección General de Tecnología de Información.

Artículo 53. El usuario que requiera de la contratación de un nombre de dominio, servicio de hospedaje o de nube, entendida ésta como los servicios de almacenamiento o de procesamiento de información a través de internet distinto al institucional, para el desempeño de sus actividades de divulgación de información institucional en el internet, debe contar con la autorización del Comité Estratégico de Tecnologías de la Información, para lo cual debe dirigir la solicitud al Secretario de Desarrollo Institucional como Secretario Ejecutivo de dicho Comité.

Artículo 54. El diseño, administración y contenido de los portales web es responsabilidad de cada titular de la entidad académica o dependencia, de acuerdo con sus requerimientos de difusión de información.

Artículo 55. Cuando se requiera alojar información reservada o confidencial en la nube, el usuario debe solicitar autorización del Comité Estratégico de Tecnologías de la Información.

Artículo 56. El usuario responsable de algún servicio de tecnología de información debe 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 57. El usuario que tenga asignado un recurso de tecnología de información y comunicación, patrimonio de la Universidad, debe 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 58. El usuario que cuente con *software* institucional de protección contra código malicioso, debe mantenerlo actualizado y respetar la configuración de seguridad del equipo asignado, para detectar y prevenir la propagación de código malicioso.

Artículo 59. 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 y comunicación institucional, debe verificar que no cuente con código malicioso mediante la ejecución de un *software* de protección actualizado.

Capítulo VII
De la ciberseguridad

Artículo 60. La ciberseguridad es el conjunto de acciones para prevenir y detectar el uso no autorizado de la infraestructura tecnológica de la Universidad Veracruzana, mitigando los riesgos que pudieran afectar total o parcialmente los procesos institucionales.

Artículo 61. Los mecanismos y estrategias para la prevención, identificación y mitigación de incidentes de ciberseguridad serán implementados por la Dirección General de Tecnología de Información, en el caso de identificarse un incidente se aplicará las Leyes en la materia.

Artículo 62. El alcance de los procesos asociados a la identificación y gestión de incidentes de seguridad se limitarán a la infraestructura tecnológica perteneciente a la Universidad Veracruzana.

Título IV De las responsabilidades y las sanciones

Capítulo I
De las responsabilidades

Artículo 63. Los integrantes de la comunidad universitaria son 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 64. 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, deben:

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 65. Cualquier integrante de la comunidad universitaria en el desarrollo de sus actividades, debe 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, la normatividad emitida por los órganos colegiados establecidos en este Reglamento.

Capítulo II
De las sanciones

Artículo 66. El usuario que transgreda las medidas de control para la seguridad de la información física o lógica establecidas en el presente Reglamento podrá ser sancionado en los términos de la legislación universitaria y las leyes aplicables en la materia.

Artículo 67. 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 pudieran ser de la competencia del Código Penal o cualquier otra legislación aplicable.

Artículo 68. 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 digital o electrónica;
II. Generar algún tipo de incidente de ciberseguridad;
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 69. 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 hábil 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 abroga el Reglamento para la Seguridad de la Información aprobado en sesión del H. Consejo Universitario General el día 14 de diciembre de 2016.

Cuarto. Publíquese, difúndase y cúmplase.

APROBADO EN SESIÓN DEL H. CONSEJO UNIVERSITARIO GENERAL CELEBRADA EL DÍA 9 DE DICIEMBRE DE 2019.

Dirección de Normatividad.