NORMA ISO 27001

Tecnología de la información

Técnicas de seguridad

Sistemas de Gestión de la Seguridad de la Información (SGSI)

Controles de seguridad de la información

REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN

Última Fecha de Actualización: Septiembre 07, 2021

UNIVERSIDAD AUTÓNOMA DE TAMAULIPAS
Matamoros SN, Zona Centro,
Cd. Victoria, Tamaulipas, México. C.P. 87000

Teléfono directo: (834) 318-1854
Conmutador: (834) 318-1800, ext. 1264.

Contenido

REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN

CAPITULO I
DISPOSICIONES GENERALES

ARTÍCULO 1. El presente reglamento de seguridad de la información tiene por objeto establecer el marco normativo para el uso adecuado de los activos de información de Universidad Autónoma de Tamaulipas, es de observancia general y obligatoria para los integrantes de la comunidad universitaria, así como las personas o usuarios externos que hagan uso de los activos de información de la misma. Además de sensibilizar, regula las medidas de control para salvaguardar la confidencialidad, integridad y disponibilidad de la información institucional.

ARTÍCULO 2. El ordenamiento cumple con los requisitos de seguridad de la información establecidos en las Norma Mexicanas NMX-I-27001-NYCE-2015 "Tecnologías de la Información - Técnicas de Seguridad - Sistemas de Gestión de Seguridad de la Información - Requisitos" y NMX-I-27002-NYCE-2015 "Tecnologías de la Información - Técnicas de Seguridad – Código de Buenas Prácticas para el Control de la Seguridad de la Información", en concordancia con las Normas Internacionales ISO/IEC 27001:2013 "Information Technology - Security Techniques - Information Security Management Systems - Requirements" y ISO/IEC 27002:2013 "Information Technology - Security Techniques – Code of Practice of Information Security Control", respectivamente.

ARTÍCULO 3. La información generada durante la jornada de laboral de funcionarios y empleados de la Universidad Autónoma de Tamaulipas, así como el personal externo que se contrate para la realización de un trabajo, obra, investigación determinada o con motivos de las funciones que desempeñe en la misma, será propiedad de la Universidad. En la explotación del resultado se aplicará lo dispuesto en la Ley Federal de Derechos de Autor, el Reglamento de Investigación y la normatividad aplicable.

ARTÍCULO 4. Para los efectos del presente reglamento, se entenderá por:

I. Acuerdo de Confidencialidad: Documento en el cual las partes firmantes se obligan a respetar el secreto y la confidencialidad de la información que se van a compartir, y a usarla sólo para el fin que se estipule en el acuerdo.

II. Código: Conjunto unitario, ordenado y sistematizado de normas y principios jurídicos.

III. Colaboradores: Personal de apoyo administrativo, estudiantes becados, de apoyo, de servicio social y de prácticas profesionales.

IV. Comité: Conjunto de personas elegidas para desempeñar una labor determinada, especialmente si tiene autoridad o actúa en representación de un colectivo.

V. Comunidad universitaria: funcionarios, empleados y estudiantes universitarios.

VI. DIAA: Dirección de Información Académica y Administrativa.

VII. DSF: Dirección de Sistemas Financieros.

VIII. DTI: Dirección de Tecnologías de la Información.

IX. Estatuto Orgánico: Los estatutos son normas jurídicas que imponen reglas de conducta (estatuyen, ordenan, establecen) en determinados ámbitos territoriales o con relación a actividades específicas.

X. GTSI: Grupo de Trabajo de Arquitectura Tecnológica, integrado por funcionarios y empleados encargados de gestionar las tecnologías de la información y seleccionar la dirección tecnológica de la Universidad Autónoma de Tamaulipas para el desarrollo de un programa de tecnología que facilite la selección, desarrollo, aplicación y uso de la infraestructura tecnológica.

XI. GTSI: Grupo de Trabajo de Seguridad de la Información, integrado por funcionarios y empleados que gestionan las tecnologías de la información encargados de coordinar, fomentar, controlar y prestar apoyo activo a la seguridad de la información en la Universidad Autónoma de Tamaulipas.

XII. Norma ISO: Las normas ISO son un conjunto de normas orientadas a ordenar la gestión de una empresa en sus distintos ámbitos. Las normas ISO son establecidas por el Organismo Internacional de Estandarización (ISO), y se componen de estándares y guías relacionados con sistemas y herramientas específicas de gestión aplicables en cualquier tipo de organización.

XIII. Norma: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

XIV. Objetivo: Fin que se quiere alcanzar y al cual se dirige una acción.

XV. Partes interesadas: Para efectos de cualquier sistema de gestión basado en una norma ISO, se considera a todas las personas u organizaciones, públicas o privadas, internas o externas, de alguna forma, aunque sea tangencial, pueden influir o impactar en el objetivo de nuestro sistema.

XVI. Política: Es un plan general de acción que guía a la organización en la conducta de su operación.

XVII. Procedimiento: Consisten en secuencias cronológicas de las acciones requeridas. Son guías de acción, no de pensamiento, en las que se detalla la manera exacta en que deben realizarse ciertas actividades.

XVIII. Proceso: Un proceso es una secuencia de pasos dispuesta con algún tipo de lógica que se enfoca en lograr algún resultado específico.

XIX. Protocolo: Conjunto de instrucciones, normativas o reglas que permiten guiar o regular una determinada acción.

XX. Proveedor: Los proveedores son aquellas empresas que abastecen a otras con bienes o servicios necesarios para el correcto funcionamiento del negocio. La palabra proveedor deriva del verbo proveer que significa suministrar, abastecer, entregar.

XXI. Proyecto: Un proyecto es un proceso desencadenado para lograr un cambio cualitativo o cuantitativo de una situación definida como problema. Supone una inversión de recursos, efectuada para alcanzar un objetivo concreto, en tiempo determinado, mediante actividades coordinadas y bajo una unidad de gerencia.

XXII. Reglamento: Conjunto ordenado de reglas o preceptos dictados por la autoridad competente para la ejecución de una ley, para el funcionamiento de una corporación, de un servicio o de cualquier actividad.

XXIII. SAIS: Sistema de Administración de Inventarios y Servicios https://sais.uat.edu.mx/ administrado por la Dirección de Tecnologías de la Información.

XXIV. Sanción: El concepto refiere a un castigo que se aplica a la persona que viola una norma o una regla.

XXV. Servicio tercerizado: La externalización de servicios o subcontratación es el proceso por el cual una empresa requiere los servicios de otra empresa externa para realizar una actividad determinada. Es una práctica que busca la eficiencia y la optimización de los recursos.

XXVI. SGSI: El Sistema de Gestión de la Seguridad de la Información de la Universidad Autónoma de Tamaulipas.

XXVII. SI: Seguridad de la Información.

XXVIII. SIGETSI: Sistema de Gestión de Tecnologías y Seguridad de la Información de la Universidad Autónoma de Tamaulipas.

XXIX. TI: Tecnologías de la Información.

XXX. Universidad: Universidad Autónoma de Tamaulipas.

ARTÍCULO 5. El Grupo de Trabajo de Seguridad de la Información es responsable de vigilar la correcta aplicación y cumplimiento del presente reglamento, así como efectuar las modificaciones o adecuaciones que se consideren necesarias.

ARTÍCULO 6. El Grupo de Trabajo de Seguridad de la Información es responsable de mantener el Sistema de Gestión de la Seguridad de la Información (SGSI) que incluye los procesos, recursos, procedimientos, controles, tecnologías y herramientas necesarias para garantizar la confidencialidad, integridad y disponibilidad de los activos de información y los activos tecnológicos que dan soporte a la Universidad, en especial a los procesos incluidos en su Alcance.

CAPITULO II
POLITICAS DE SEGURIDAD DE LA INFORMACION

ARTÍCULO 7. El Grupo de Trabajo de Seguridad de la Información deberá comunicar a la comunidad universitaria y partes interesadas, la política de seguridad de la información institucional aprobada por la Rectoría, de manera que sea relevante, accesible y comprensible, comprometiéndose en implementar, mantener y mejorar la política, así como velar por el cumplimiento de la misma.
Política de Seguridad de la Información Institucional:

> *"Para lograr una administración efectiva, moderna que genere resultados eficientes y eficaces, la Universidad Autónoma de Tamaulipas reconoce que los activos de información y la infraestructura tecnológica que los soporta, son esenciales para la continuidad de los procesos y servicios tecnológicos institucionales; por lo que se compromete a identificar y proteger su acceso, uso y divulgación, cumpliendo con los requerimientos de integridad, disponibilidad y confidencialidad para disminuir el impacto de amenazas o desastres; esto con el fortalecimiento en el desarrollo de capacidades del personal que gestiona las tecnologías de la información y la mejora continua de los procesos del Sistema de Gestión de la Seguridad de la Información".*

ARTÍCULO 8. El Grupo de Trabajo de Seguridad de la Información deberá aplicar y dar cumplimiento a las siguientes directrices:

I. La información donde la universidad es propietaria y/o depositaria deberá ser accesible únicamente por personal debidamente autorizado.

II. La Política de Seguridad de la Información, así como el resto de la normatividad del SGSI, deberá ser accesible a toda la comunidad universitaria, así como el personal externo que se relaciona con éste a través de alguno de sus procesos.

III. La universidad debe cumplir con todos aquellos requerimientos legales, regulatorios y estatuarios que le sean de aplicación, así como los requerimientos contractuales.

IV. La confidencialidad de la información debe garantizarse en todo momento.

V. La integridad de la información debe asegurarse a través de todos los procesos que la gestionan, procesan y almacenan.

VI. La disponibilidad de la información debe garantizarse mediante las adecuadas medidas de respaldo y continuidad del negocio.

VII. Todo el personal dentro del alcance del SGSI de la universidad, debe disponer de la adecuada formación y concienciación en materia de seguridad de la información.

VIII. Todo incidente o debilidad que pueda comprometer o haya comprometido la confidencialidad, integridad y/o disponibilidad de la información debe ser registrado y analizado para aplicar las correspondientes medidas correctivas y/o preventivas.

ARTÍCULO 9. La violación por acción y omisión de este ordenamiento implica, actualiza y/o genera sanciones en término de la normatividad aplicable. La supervisión del adecuado cumplimiento estará a cargo de los órganos de vigilancia de la Universidad tal y como lo establece el estatuto orgánico institucional.

ARTÍCULO 10. El Grupo de Trabajo de Seguridad de la Información deberá difundir las políticas internas de seguridad de la información sobre el control de acceso, cuyo objetivo es limitar el acceso a la información y a las instalaciones de procesamiento de la información, aplicado a todo el personal de las áreas que gestionan tecnologías de la información en la universidad, así como personal externo contratado para servicios tercerizados que hagan uso de la infraestructura, plataformas tecnológicas y los sistemas de información de la universidad, que le sea asignado o haga uso de equipos portátiles, dispositivos móviles propiedad de la universidad y deberán cumplirse conforme lo establecido.

La asignación y el uso de los derechos de acceso privilegiado deben restringirse y controlarse. En caso de autorización se recomienda que la asignación sea acorde a la necesidad de uso o por evento especificando el tiempo de expiración del acceso, revisando periódicamente que los accesos de los usuarios privilegiados correspondan con las funciones a desempeñar. Además, se sugiere considerar:

I. Aspectos generales. –

a. Todo acceso está restringido a menos que este expresamente permitido.
b. Identificar y registrar el acceso a los servicios de red y sistemas operativos o aplicaciones.
c. Utilizar mecanismos de autenticación para el acceso a redes de la universidad como validación por dominio, usuario y/o contraseña.
d. Retirar los accesos de personal que dejen de laborar en la universidad.
e. Revisar los accesos cada 6 meses, después de cambios mayores o cuando se produzca un incidente de seguridad.
f. Retirar los accesos cuando se considere que la seguridad de la información está comprometida.
g. Permitir la verificación del cumplimiento de esta política por el área de Seguridad de la Información en la Coordinación de Informática y Telecomunicaciones dependiente de la Dirección de Tecnologías de la Información o área afín en otra dependencia que realiza la verificación.

II. Acceso a Red. -

a. Utilizar el protocolo de seguridad WPA2 o superior en redes inalámbricas.

b. Restringir el acceso o descarga de archivos en sitios conectados punto a punto.

c. Restringir el acceso a redes internas a personal externo.

III. Acceso a Sistemas Operativos o Aplicaciones. -

a. Restringir los privilegios de administrador a usuarios finales.

b. No permitir la creación de usuarios genéricos para el acceso privilegiado (administradores) a servidores u aplicaciones críticas.

c. Asegurar el uso de procedimientos de inicio seguros de sesión:

1. Asegurar que no se proporcione el acceso hasta que todos los datos de entrada se hayan ingresado y validado.
2. Evitar proporcionar mensajes de ayuda durante el proceso de autenticación.
3. Limitar el número de intentos fallidos.
4. Evitar la visualización de contraseñas digitadas dentro de los sistemas.

IV. Gestión de contraseñas o información secreta de autenticación. -

a. Utilizar mecanismos seguros para la creación de contraseñas:

1. La longitud de contraseñas debe ser de al menos ocho (8) caracteres.
2. Utilizar mecanismos alfanuméricos.
3. Evitar palabras que sean fáciles de adivinar como: 12345, fecha de nacimiento, etc.

b. Evitar el envío de contraseñas en texto plano.

c. Forzar el cambio de contraseñas al menos una vez cada seis (6) meses.

d. Registrar las actividades del personal que proporciona acceso privilegiado.

e. Limitar el uso de redes, aplicaciones o sistemas a un número mínimo necesario de usuarios de confianza.

V. Responsabilidad de uso de contraseñas o información secreta de autenticación. -

a. No habilitar la función de “recordar contraseñas”.

b. No compartir contraseñas.

c. No guardar las contraseñas en lugares fácilmente identificables.
d. Mantener secreta la información de autenticación.
e. Cambiar la información secreta de autenticación siempre que exista un indicio de riesgo.

ARTÍCULO 11. El Grupo de Trabajo de Seguridad de la Información difundirá la Política de Teletrabajo y las políticas internas de seguridad de la información sobre el Escritorio y Pantalla Limpia con el objeto de proteger la información que se maneja en los equipos de escritorio y portátiles, y lugares de trabajo a distancia contra posibles riesgos como: mal uso, robo, modificación, entre otros.
Se recomienda que los equipos de escritorio, portátiles y lugares de trabajo de todos los colaboradores y gestores de tecnologías de la información y demás personal se mantengan libres de cualquier tipo de información para evitar su mal uso, y en caso de ser información sensible, resguardarse conforme a la Política de Clasificación de la Información, establecida en el artículo 15 de este reglamento. Además, se sugiere considerar:

I. Sobre el mobiliario. -

a. La Secretaría de Administración por conducto de la Coordinación General de Proyectos de Infraestructura es la responsable de diseñar la ubicación de los lugares de trabajo de la universidad de tal forma que se minimice el riesgo de acceso de personas externas a la institución.
b. La Secretaría de Administración por conducto de la Dirección de Control Patrimonial provee al personal y a los colaboradores los muebles de acceso controlado necesarios, tales como: gabinetes, cajoneras, entre otros.

II. Sobre los equipos de escritorio, portátiles y lugares de trabajo. -

a. Cuando un colaborador se ausente de su lugar de trabajo, bloquear su estación de trabajo y guardar en un lugar seguro cualquier documento, medios de almacenamiento que contenga información institucional.
b. Al finalizar la jornada laboral, el colaborador guardará en un lugar seguro los documentos y medios de almacenamiento que contengan información sensible, confidencial o reservada, además de desconectarse o cerrar sesión de los sistemas de información de la universidad.
c. Los colaboradores que, por funciones del puesto, cuenten con oficina, la cerrarán con llave cada vez que se ausenten de su lugar de trabajo.
d. Los colaboradores mantendrán sobre su lugar de trabajo la información mínima indispensable para realizar sus actividades, evitando en todo momento dejar a la vista información reservada o confidencial.

III. Sobre las pantallas de los equipos de escritorio y portátiles. -

a. El área responsable de infraestructura correspondiente deberá configurar los equipos de escritorio y portátiles de los colaboradores para que se active el protector de pantalla y desbloqueo con contraseña, después de un periodo de cinco (5) minutos de inactividad.
b. Retirar inmediatamente de las impresoras medios que contengan información clasificada.

Todo el personal del alcance del SGSI que tenga la responsabilidad de realizar y vigilar operaciones tecnológicas desde lugares de trabajo remoto dentro y fuera del horario laboral y dar seguimiento a las actividades asignadas y de servicios que son esenciales para la dirección darán cumplimiento en lo establecido en la Política de Teletrabajo.

ARTÍCULO 12. El Grupo de Trabajo de Seguridad de la Información difundirá las políticas internas de seguridad sobre la transferencia de información, con el objeto mantener la seguridad de lo que se transmita a través de la red de datos de la universidad o escrita a cualquier entidad externa, como se recomienda a continuación:

I. Transferencia de Información a Proveedores o Clientes. -

a. En la medida de lo posible evitar el envío de información sensible o crítica a personal externo a la universidad.
b. Firmar un acuerdo de confidencialidad y transferencia de información sensible o crítica cuando se envíe a personal externo a la universidad.

II. Transferencia de Información Digital o Electrónica. –

a. Entregar de manera personal la transferencia de información sensible o crítica, validar la autorización e identidad de la persona quién recibirá la información.
b. Definir las herramientas para el envío de información de uso interno que cuenten con mecanismos de acceso y privilegios.
c. Uso de cifrado para la protección de la información confidencial que viaja por canales seguros de las comunicaciones, tales como SSL/TLS, VPN, IPSec, SSH u otros, incluyendo el uso de gestión de certificados, tokens o llaves para estos fines.
d. Proporcionar la información secreta de autenticación vía telefónica, no dejar esa información en contestadoras telefónicas ni buzones.
e. Evitar el uso de memoria USB y cualquier medio extraíble en los puertos de USB del equipo propiedad de la universidad. En caso de utilizar este medio, deberá analizar el dispositivo extraíble para detectar y proteger la información y el equipo de cómputo contra software malicioso (virus, malware, etc.).

III. Transferencia de información física. –

a. Enviar la información de uso interno por los mecanismos autorizados por la Universidad.
b. Proteger la información utilizando un sobre cerrado, sin referencias sobre su contenido.

ARTÍCULO 13. El personal que gestiona seguridad de la información de la universidad deberá evitar mantener conversaciones confidenciales en lugares públicos o en canales de comunicación no seguros, oficinas abiertas o lugares de reunión.

ARTÍCULO 14. El Grupo de Trabajo de Seguridad de la Información difundirán las recomendaciones en el uso de dispositivos móviles y equipos portátiles, con el objeto de proteger la información que se maneja en la infraestructura tecnológica de cómputo y almacenamiento propiedad de la universidad, para lo cual se sugiere cumplir con las medidas de seguridad señaladas a continuación:

Tener cuidado con el uso de dispositivos móviles en lugares públicos o áreas no protegidas, para evitar el acceso no autorizado o la divulgación de la información almacenada y procesada, crítica o sensible y contar con sistemas de bloqueo especiales que sean utilizados para asegurar dichos dispositivos.
Concientizar al personal de seguridad de la información sobre los riesgos derivados y de los controles que se necesitan implementar.
Se recomienda que cualquier equipo móvil que contenga información de la universidad cumpla con las siguientes medidas de seguridad:

I. Laptops o tabletas.

- Activar el bloqueo del equipo y el acceso mediante contraseña.
- Contar con un antivirus actualizado.
- Es recomendable mantener actualizado el sistema operativo genuino del dispositivo, siendo descargado del sitio de la casa de software original.
- Se recomienda implementar controles adicionales para proteger la información personal o clasificada como critica/sensible en el equipo, por ejemplo, cifrado del disco duro de equipo, proteger el acceso al documento mediante contraseñas entre otros.
- Se recomienda mantener un respaldo de la información crítica basado en la Política de Respaldos de la Información.
- No dejar el equipo en lugares que puedan ser susceptibles a robo (en lugares visibles dentro del auto, en lugares públicos cafeterías, eventos, conferencias).
- No cargar los dispositivos móviles en puertos de USB públicos.
- Evitar la conexión mediante redes WiFi en lugares públicos y de aquellas conexiones que no cuenten con un control de acceso.

- Se recomienda el uso de correo electrónico de la universidad (institucional), siempre que cuente con credenciales de autentificación de usuario (Alumnos activos, docentes, investigadores, personal administrativo), el acceso a la red interna o sistemas de información de la universidad está prohibido por este medio, a menos que cuente con permiso expresamente para este propósito. Si utiliza un correo electrónico gratuito adicional en el dispositivo, se recomienda extremar precauciones debido a la propagación de virus y malware, así como la recepción constante de correos phishing que incluyen el riesgo de seguridad de la información.
- Es responsabilidad del personal el correcto uso del servicio de acceso remoto que haga conexión vía VPN, asegurando de no compartir su cuenta de acceso, quedando sujetos a lo establecido a las normas y políticas sobre el uso de la tecnología y equipos propiedad de la universidad.

II. Telefonía Móvil.

- Es recomendable evitar cargar los dispositivos móviles en puertos de USB públicos.
- Se recomienda mantener un respaldo de la información crítica basado en la Política de Respaldos de la Información.
- Contar con un antivirus actualizado.
- Es muy recomendable activar el acceso mediante Número de Identificación Personal NIP – PIN por sus siglas en inglés, el cual se solicita cuando se reinicia el equipo o se cambia el chip.

- Se recomienda el uso de correo electrónico de la universidad (institucional), siempre que cuente con credenciales de autentificación de usuario (Alumnos activos, docentes, investigadores, personal administrativo), el acceso a la red interna o sistemas de información de la universidad está prohibido por este medio, a menos que cuente con permiso expresamente para este propósito. Si utiliza un correo electrónico gratuito adicional en el dispositivo, se recomienda extremar precauciones debido a la propagación de virus y malware, así como la recepción constante de correos phishing que incluyen el riesgo de seguridad de la información.
  - El acceso a la red interna o sistemas de la universidad está prohibido por este medio, a menos que cuente con permiso expresamente para este propósito.
  - Es recomendable mantener actualizado el software del dispositivo, siendo descargados de sitios de la casa de software original o de confianza.
  - Es recomendable evitar utilizar el equipo como medio de almacenamiento de información de la universidad.
  - Es recomendable mantener inhabilitada la sesión de inicio de credenciales, que permitan el “recordar contraseña o conexiones de red universitaria” que impida a usuarios no autorizados el acceso a la información de la universidad.
- Es recomendable evitar tomar fotos y/o vídeo a contenido confidencial de la universidad (documentos, áreas de oficinas, pantallas de sistemas, etc.)
- Es recomendable hacer uso del temporizador de bloqueo de pantalla, esto evitará que usuarios no autorizados tengan acceso directo a las aplicaciones y archivos, salvaguardando significativamente la confidencialidad e integridad de la información de la universidad.

- Es recomendable realizar encriptación del dispositivo móvil sobre los datos almacenados en la memoria no volátil, cuyo fin es proporcionar confidencialidad de la información.
- Es recomendable mantener apagada la conexión Bluetooth cuando no se esté utilizando, esto para impedir virus y conexiones no autorizadas que comprometan la integridad y confidencialidad de los datos.
- Es recomendable cerrar las sesiones iniciadas al terminar de usarlas.
- Evitar compartir o prestar el equipo móvil, reduciendo considerablemente la disponibilidad de información que pueda comprometerse.
- Es recomendable realizar periódicamente (tiempos) limpieza segura mediante borrado remoto, cuyo fin es prohibir el acceso directo al dispositivo e intentando asegurar que los datos ya no están en riesgo.
- Es recomendable guardar el número IMEI (Identidad Internacional de Equipo Móvil) para en caso de robo para inutilizar el móvil.

III. Medios Removibles Personales

- Evitar el uso de memoria USB y cualquier medio extraíble.
- Se recomienda rescindir del uso de memoria USB, y evitar cualquier medio extraíble en los puertos de USB del equipo propiedad de la universidad.

ARTÍCULO 15. El Grupo de Trabajo de Seguridad de la Información difundirá las políticas internas de clasificación de la información, con el objeto de clasificar los activos de la información para garantizar una eficaz gestión de su seguridad con criterios de confidencialidad, integridad y disponibilidad. Dicha clasificación debe realizarse en términos de su valor, requisitos legales, sensibilidad o criticidad.
Los activos de información propiedad de la universidad y/o en su custodia que se encuentren dentro del Alcance del SGSI, se clasificarán de acuerdo con los niveles definidos en la Matriz de Clasificación de la Información y los Lineamientos generales para la administración y conservación de archivos del SGSI. La clasificación y controles de protección asociados a la información tomarán en cuenta las necesidades específicas de la institución con respecto a la distribución (uso compartido) o restricción de la información, así como las obligaciones de resguardo de información que le impone a la universidad la normativa estatal y nacional.
La responsabilidad por la clasificación de un ítem de información y por la revisión periódica de dicha clasificación, recae en el creador o responsable asignado de la información dentro de los criterios de clasificación aprobados por la universidad. La clasificación deberá mantenerse actualizada en todo momento.

I. El tipo de información a clasificar es:

a. Documental. - Material escrito en papel o formato electrónico.
b. Infraestructura. - Bienes, servicios e instalaciones de un edificio.
c. Salas. - Espacio físico o virtual destinado para realizar reuniones de personas.
d. Consola de administración. - Software operado por el administrador para gestionar los recursos de infraestructura tecnológica.
e. Software. - Programas destinados para ser instalados en equipo PC de usuario final.

f. Suscripción. - Bien o servicio informático que se paga a un tercero para ser accedido desde internet.

g. Sistema de información. - Aplicación web desarrollada para una parte interesada de la UAT.

h. Repositorio. - Espacio físico o virtual para almacenar archivos.

II. Los niveles de clasificación de la información son:

a. Confidencial. - Toda información que de ser revelada sin autorización o manejada por entes no autorizados, puede causar graves daños a la universidad, los administrados, funcionarios y/o aliados institucionales. El uso de este tipo de información requerirá de previa autorización por parte del responsable asignado de la misma e incluso la suscripción de acuerdos de confidencialidad para mayor protección.
Esta clasificación incluye información altamente sensible de la universidad. Información que los alumnos, docentes, funcionarios, personal de confianza y sindicalizado proporcionan a la institución.

b. Reservada. - Es aquella información que es única y exclusivamente para uso interno de la universidad. Esta información incluye toda aquella información que requiere de un nivel de protección que cumple con los criterios necesarios para ser reservada.

Esta clasificación incluye información de uso general solo para los empleados y protegida del acceso externo.

c. Pública. - Es toda aquella información que se genera para su divulgación pública. Para esta información sólo se deben de implementar los controles adecuados para asegurar la integridad y disponibilidad de la misma.

Esta clasificación incluye información que puede ser conocida y utilizada por personal interno y/o externo.

Definir valores de criticidad de la información en la Matriz de Clasificación de la Información con base en los criterios de confidencialidad, integridad y disponibilidad.
Definir el grado de disponibilidad de los activos de información dependiendo de su posible alteración o destrucción:

CAPITULO III
DE LOS RECURSOS HUMANOS

ARTÍCULO 16. En el caso de los aspirantes a un puesto vacante en las áreas que gestionan tecnologías de la información o en las áreas de las partes interesadas consideradas dentro del Alcance del SGSI, se llevará a cabo una revisión documental del currículum vitae, cédula o Título (ambos, si ya cuenta con ellos) profesional, de las capacitaciones y/o certificaciones que garanticen las competencias, habilidades y aptitudes, referencias laborales y la evaluación de la experiencia de conformidad al puesto vacante. La Carta de No Antecedentes Penales es facultad de las Direcciones de Recursos Humanos y Nominas solicitarla y validarla.
ARTÍCULO 17. Para el personal de nuevo ingreso en las áreas que gestionan tecnologías de la información o en las áreas de las partes interesadas consideradas dentro del Alcance del SGSI, los trámites correspondientes para su selección, términos y condiciones de la relación laboral, proceso disciplinario, derechos y obligaciones legales, se sujetarán a lo establecido en la normatividad institucional vigente que emita la Dirección de Recursos Humanos.
Es responsabilidad del área de adscripción en colaboración con el Grupo de Trabajo de Seguridad de la Información la concientización y capacitación en seguridad de la información.
ARTÍCULO 18. Los titulares de las áreas que gestionan tecnologías de la información deberán comunicar y difundir al personal a su cargo, las funciones y el nivel jerárquico que ocupan dentro de la estructura organizacional.
Asimismo, deberán asegurar que el personal comprenda y se comprometa a desarrollar sus funciones, que mantenga un adecuado código de conducta en las relaciones laborales, un uso adecuado de la infraestructura tecnológica y de las instalaciones institucionales; los puestos serán asignados con base en los acuerdos de contratación.
Es compromiso de las áreas de adscripción asegurarse que su personal se concientice y cumpla con los roles y responsabilidades establecidas en el SGSI y sus políticas de seguridad de la información.
ARTÍCULO 19. El Grupo de Trabajo de Seguridad de la Información deberá establecer e implementar un programa de concientización para la seguridad de la información alineado a la política y objetivos de seguridad de la información del SGSI.
ARTÍCULO 20. El personal de las áreas que gestionan tecnologías de la información y las áreas de las partes interesadas consideradas dentro del Alcance del SGSI, que tenga acceso a información confidencial o reservada, firmarán un acuerdo de confidencialidad y no divulgación.
ARTÍCULO 21. En caso de baja de personal, el titular del área se encargará de ejecutar el proceso de la baja administrativa con las autoridades correspondientes y en base a lo establecido en los Lineamientos de la Gestión de la Cuenta Institucional Para Empleados y en la Guía de Gestión de Acceso del Usuario.

I. Cuando la baja está autorizada, el titular realizará las siguientes acciones:

    1. Suspender las credenciales institucionales y accesos a los servicios tecnológicos correspondientes del empleado.

    2. Ejecutar el procedimiento de eliminación y borrado seguro al equipo de tecnologías de la información de la institución y/o a su equipo personal.

    3. Revisar que cualquier dato sensible y software licenciado haya sido eliminado o sobrescrito de manera segura previo a su reutilización.

4. Gestionar la devolución de los activos a su cargo al área correspondiente y actualizar la información en el inventario de la universidad.

5. En caso de cambio de puesto, el titular del área se encargará de gestionar que se realicen los cambios en los permisos de acceso de acuerdo con la función del puesto y activos de información.

CAPÍTULO IV
GESTIÓN DE ACTIVOS

ARTÍCULO 22. Los Grupos de Trabajo de Seguridad de la Información y de Arquitectura Tecnológica deberán identificar los activos de información dentro del Alcance del SGSI, definir los controles de seguridad de la información necesarios a fin de minimizar el impacto a la universidad por incidentes o riesgos que se materialicen al interior de los mismos o en su entorno, en los centros de datos y en las instalaciones donde se gestionan las tecnologías de la información.
Este inventario deberá incluir toda la información necesaria del activo de información y sus componentes entre otros elementos de acuerdo con lo establecido en el SIGETSI.
ARTÍCULO 23. El Grupo de Trabajo de Seguridad de la Información aplicará y hará cumplir la política de clasificación de información descrita en el artículo 15.
ARTÍCULO 24. La Dirección de Tecnologías de la Información administra, controla y actualiza el inventario de activos de información y tecnológicos por medio de la herramienta tecnológica del Sistema de Administración de Inventarios y Servicios - SAIS https://sais.uat.edu.mx/.
ARTÍCULO 25. La Dirección de Control Patrimonial es la encargada de mantener permanentemente actualizado el inventario de bienes de la universidad llevando el registro individual de cada bien y asignando un número de control a los mismos.
ARTÍCULO 26. La Dirección de Tecnologías de la Información es la encargada de la asistencia y soporte técnico de los activos de información y tecnológicos de la universidad, del control de garantías de los activos de software, de su vigilancia y del registro de los servicios de TI, por medio de la herramienta tecnológica SAIS.
ARTÍCULO 27. El Grupo de Trabajo de Seguridad de la Información por conducto de las áreas responsables de gestionar el SGSI, mantendrán un registro de las evidencias de eliminación de datos o información sensible que se almacenan en los activos de información incluidos en el Alcance del SGSI.

CAPÍTULO V
SEGURIDAD FÍSICA Y AMBIENTAL

ARTÍCULO 28. El Grupo de Trabajo de Seguridad de la Información por conducto de las áreas responsables de gestionar el SGSI, podrá establecer controles de seguridad física en los centros de datos y en las áreas donde se gestionan tecnologías de la información, así como para el acceso a dichos espacios, a sus componentes o elementos del ambiente operativo como lo establece el SGSI.

ARTÍCULO 29. El Grupo de Trabajo de Seguridad de la Información por conducto de las áreas responsables de gestionar el SGSI, podrá establecer puntos de control de acceso físico que incluya un registro y la entrega de un gafete para los visitantes y/o personal que atiende servicios tercerizados, el filtro solo permita el ingreso de personas autorizadas.

ARTÍCULO 30. El Grupo de Trabajo de Seguridad de la Información por conducto de las áreas responsables de gestionar el SGSI, podrá instalar sistemas de alarmas para la medición de temperatura, humedad, detección de humo, contra incendios y de video vigilancia para prevenir la perdida, daño o robo; operar de manera coordinada con la Dirección de Protección Universitaria, Protección civil, bomberos y autoridades locales, estatales y federales.

ARTÍCULO 31. El Grupo de Trabajo de Seguridad de la Información por conducto de las áreas responsables de gestionar el SGSI, deberá asegurar y proteger los activos de información, reducir los riesgos de amenazas internas, externas, ambientales, fallas de energías y/o interrupciones causadas por los servicios públicos, previniendo la pérdida, daño o robo de los activos de información, en caso de afectación deberán contar con un plan de continuidad.

CAPITULO VI
SEGURIDAD EN LAS OPERACIONES

ARTÍCULO 32. El Grupo de Trabajo de Seguridad de la Información por conducto de las áreas responsables de gestionar el SGSI, podrá implementar el proceso de Operación de Infraestructura del SIGETSI para:

I. Entregar a los usuarios, los servicios de TI conforme a los niveles de servicio acordados y con los controles de seguridad definidos.

II. Implementar en los Centros de datos y áreas críticas, las condiciones de operación de infraestructura, así como los controles necesarios a fin de minimizar el impacto a la universidad por incidentes o riesgos que se materialicen al interior de los mismos o en su entorno.

III. Mantener actualizada la infraestructura tecnológica para garantizar la continuidad de los servicios de TI.

ARTÍCULO 33. El Grupo de Trabajo de Seguridad de la Información por conducto de las áreas responsables de gestionar el SGSI, deberá contar con una política de respaldos que defina los requisitos de la conservación y de la protección de la información del software y los sistemas que incluya entre otros lo siguientes:

I. Registro de los respaldos y su restauración.

II. Almacenamiento aislado de los respaldos, protección física y ambiental de la información respaldada de acuerdo con las políticas establecidas.

III. Realizar pruebas de monitoreo para verificar la integridad del respaldo.

IV. Proteger mediante el cifrado la información respaldada, en el caso de los sistemas que los respaldos cubran la totalidad de la información, aplicaciones y datos necesarios para su recuperación completa.

ARTÍCULO 34. El Grupo de Trabajo de Seguridad de la Información por conducto de las áreas responsables de gestionar el SGSI, deberá prevenir la explotación de vulnerabilidades técnicas, obteniendo información sobre la seguridad de aquellos sistemas de información que puedan encontrarse vulnerables, evaluar la exposición de la organización a tales vulnerabilidades y tomar medidas apropiadas para tratar los riesgos asociados hasta su remediación, recomendando establecer un plan de acción apropiado y oportuno para la identificación de las posibles vulnerabilidades.

CAPITULO VII
ADQUISICIÓN Y DESARROLLO Y MANTENIMIENTO DE SISTEMAS

ARTÍCULO 35. En la adquisición de sistemas de información o mejoras a los sistemas de información existentes se deberá garantizar que los contratos con los proveedores contengan los requisitos de seguridad de la información como parte integral, revisando cualquier funcionalidad adicional para asegurarse de que no presenta riesgos adicionales.
ARTÍCULO 36. Los servicios sobre aplicaciones en redes deberán incluir lo siguiente:

- Procesos de autorización asociados con quienes puedan aprobar el contenido, emitir o firmar documentos transaccionales clave.
- Determinar y cumplir los requisitos de confidencialidad, integridad, de prueba de envío y recepción de documentos clave.
- Revisar el nivel de confianza en la integridad de los documentos clave.
- Confidencialidad e integridad de la orden de transacción, información de pago, dirección de entrega y confirmación de ingresos.
- Evitar la pérdida o duplicidad de información de la transacción.

ARTÍCULO 37. Los acuerdos de servicios de aplicaciones deberán estar soportados por un contrato que comprometa a las partes en los términos acordados. Y que las transacciones deben estar protegida para prevenir transmisión incompleta, errores de enrutamiento, alteración de mensajes y divulgación no autorizados.
Consideraciones de seguridad de la información:

- Uso de firma electrónica por cada una de las partes involucradas en la transacción.
- Información de autenticación secreta del usuario validada y verificada
- Mantener privacidad con todas las partes involucradas
- Encriptar los protocolos para comunicarse entre todas las partes involucradas
- Seguridad de los protocolos utilizados para la comunicación entre las partes involucradas.
- Encontrarse el almacenamiento de las transacciones fuera de todo acceso público

ARTÍCULO 38. El Grupo de Trabajo de Seguridad de la Información por conducto de las áreas responsables de gestionar el SGSI, podrán establecer y aplicar reglas para el desarrollo de software y sistemas de información garantizando que la seguridad de la información se diseña e implementa en el ciclo de vida correspondiente, y que cuente con personal altamente capacitado en su uso.
ARTÍCULO 39. Cuando se realicen cambios en los sistemas de la información dentro del ciclo de vida del desarrollo, el Grupo de Trabajo de Seguridad de la Información por conducto de las áreas responsables de gestionar el SGSI, documentarán y aplicarán los procedimientos formales para asegurar la integridad de los sistemas, aplicaciones y productos, desde el diseño hasta los mantenimientos posteriores, considerando la valoración de los riesgos, análisis de los impactos y los controles de seguridad necesarios.
ARTÍCULO 40. Los procedimientos de cambio deberán incluir los siguientes requisitos:

I. Mantener un registro de los niveles de autorización acordados.

II. Asegurarse que los cambios son enviados por usuarios autorizados.

III. Identificar el software, información, base de datos y hardware donde se aplicará la modificación

IV. Identificar y verificar el código crítico de seguridad para minimiza la probabilidad de fallas.

V. Garantizar que la documentación del sistema se actualiza al terminar el cambio y que la anterior se archiva o se elimina.

VI. Mantener un control de versiones de las actualizaciones del software

VII. Asegurarse que la aplicación de los cambios se haga en el tiempo adecuado sin perturbar los procesos.

ARTÍCULO 41. Los paquetes de software suministrados por los proveedores deberán ser utilizados sin modificación de ningún cambio.

ARTÍCULO 42. Para el desarrollo de sistemas subcontratados. Se deberá supervisar y monitorear la actividad del desarrollo considerando lo siguiente:

I. Acuerdos de licenciamientos.

II. Derechos de autor y propiedad intelectual sobre el código, su contenido o funcionalidad.

III. Requisitos contractuales para las prácticas de diseño seguro, codificación y pruebas, provisión del modelo de amenaza aprobado para el desarrollador externo, evidencias de pruebas para proteger contra el contenido malicioso intencional y no intencional, presencia de vulnerabilidades; hasta su entrega y la documentación de la construcción de productos finales.

ARTÍCULO 43. Establecer programas de pruebas de aceptación y criterios relacionados a los nuevos sistemas de la información, actualizaciones y nuevas versiones, protegiendo y controlando cuidadosamente los datos de prueba y su alcance sea proporcional a la importancia y naturales del sistema, evitar el uso de datos personales operacionales que contengan información personal o cualquier información confidencial.

ARTÍCULO 44. La Universidad por conducto de la Dirección de Adquisiciones es la única facultada para convocar, adjudicar y contratar adquisiciones, arrendamientos o servicios con fundamento en el Reglamento de Adquisiciones en su capítulo segundo de la licitación pública.

CAPITULO VIII
RELACIÓN CON PROVEEDORES

ARTÍCULO 45. Garantizar la correcta protección de los activos de información en las áreas que gestionan Tecnologías de la Información, que sea accesible a los proveedores previniendo los riesgos asociados que se puedan presentar.

ARTÍCULO 46. El Grupo de Trabajo de Seguridad de la Información por conducto de las áreas responsables de gestionar el SGSI, deberá establecer un proceso de registro, control de acceso y seguimiento a proveedores y visitantes, haciendo de su conocimiento la normatividad aplicable. Además, podrá dar cumplimiento al proceso de administración de proveedores establecido en el SIGTESI.

CAPITULO IX
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 47. El Grupo de Trabajo de Seguridad de la Información por conducto de las áreas responsables de gestionar el SGSI, deberá establecer los criterios y las responsabilidades para asegurar la correcta comunicación interna, así como regular y asegurar la comunicación externa entre la Universidad Autónoma de Tamaulipas, y demás partes interesadas (usuarios de los sistemas de información y servicios tecnológicos universitarios, proveedores, contratistas, organismos superiores, entes gubernamentales, trabajadores y gestores de tecnologías de la información entre otros); relativas al SGSI.

ARTÍCULO 48. El Grupo de Trabajo de Seguridad de la Información por conducto de las áreas responsables de gestionar el SGSI, son las áreas responsables del suministro de los recursos para ejecutar los parámetros establecidos en su procedimiento. El coordinador del SGSI es el encargado de divulgarlo y verificar su cumplimiento. Será obligación de todos los trabajadores o cualquier persona que tenga vínculo o que desarrolle actividades en nombre de la universidad, el aplicar las pautas determinadas en el presente ordenamiento.

ARTÍCULO 49. Se deberán reportar los eventos y/o debilidades de seguridad de la información a través de canales de gestión apropiados y definir quién será el punto de contacto para reportar los eventos, debiendo incluir en el reporte: Los controles ineficaces de seguridad, incumplimiento a las expectativas de los principios de seguridad de la información (confidencialidad, integridad y disponibilidad), políticas o lineamientos y su mal funcionamiento.

ARTÍCULO 50. Es indispensable contar con un equipo de respuesta de incidentes de seguridad de la información, que colabore en el análisis de las causas y la obtención de resultados por medio de la evaluación de los incidentes, documentando las acciones realizadas como referencia y evidencias de futuras verificaciones.

ARTÍCULO 51. El Grupo de Trabajo de Seguridad de la Información por conducto de las áreas responsables de gestionar el SGSI, deberá establecer mecanismos de seguridad de la información que permitan medir y monitorear los eventos y debilidades e identificar si los incidentes son de alto impacto o recurrentes, realizando mejoras con controles más específicos y disminuir la frecuencia.

ARTÍCULO 52. El Grupo de Trabajo de Seguridad de la Información por conducto de las áreas responsables de gestionar el SGSI, deberá definir y aplicar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia de los resultados de los incidentes, en concordancia con los diferentes tipos de medios y dispositivos. Estos procedimientos consideraran entre otros lo siguientes datos:

I. La seguridad de las pruebas y del personal.
II. El puesto y responsabilidades del personal involucrado.
III. Sus competencias profesionales, descripción de las actividades
IV. Flujo de comunicación interna y externa
V. Medios de comunicación, reuniones informativas y su respectiva documentación.

CAPITULO X
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

ARTÍCULO 53. Establecer, implementar, documentar y mantener los procesos, procedimientos y controles para garantizar la continuidad de seguridad de la información durante situaciones adversas, asegurando una estructura de gestión adecuada para preparar mitigar y responder ante el evento contando con el personal de competencias necesarias y con autoridad para la gestión de los incidentes.

ARTÍCULO 54. Verificar los controles de continuidad de seguridad de la información a través de pruebas de funcionalidad, de conocimiento y de la rutina para operar los procesos, procedimientos y controles, asegurando que su desempeño es consistente con los objetivos. Intentar mantener un nivel de servicios, establecer un periodo de recuperación mínimo para garantiza la continuidad, recuperar la situación inicial de los servicios y procesos y analizar los resultados de aplicación del plan.

ARTÍCULO 55. El Plan de Continuidad de Seguridad de la Información deberá contener por lo menos los siguientes apartados: Definición de situaciones críticas, establecimiento de un Comité de Seguridad de la Información que será el encargado de gestionar la situación de crisis ante una incidencia, definición de posibles situaciones (situación que provoca una incidencia, acciones y secuencias sobre los incidentes y mantener los registros para su posterior análisis y realización de acciones de mejora.

ARTÍCULO 56. Para desarrollar un plan de contingencia de seguridad de la información es necesario seguir las siguientes fases:

I. Definición del proyecto. - Objetivos, alcance y escenario.
II. Análisis de impacto. - Análisis del riesgo evaluar, el impacto del incidente, e identificar procesos, activos críticos y asignar el tiempo de recuperación.
III. Selección de estrategias. - evaluar ventajas y desventajas.
IV. Desarrollo de planes. - pruebas y mantenimiento.

CAPITULO XI
CUMPLIMIENTO

ARTÍCULO 57. El Grupo de Trabajo de Seguridad de la Información por conducto de las áreas responsables de gestionar el SGSI, evitarán brechas de obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con la seguridad de la información y cualquier requisito de seguridad.

ARTÍCULO 58. El Grupo de Trabajo de Seguridad de la Información por conducto de las áreas responsables de gestionar el SGSI, garantizarán que la seguridad de la información se implemente y opere de acuerdo a las políticas, objetivos y procedimientos institucionales, debiendo hacer revisiones planeadas o cuando ocurran cambios significativos con el objetivo de asegurar la continuidad del Sistema de Gestión de la Seguridad de la Información.

En caso de incumplimiento como resultado de la revisión, el GTSI deberá:

I. Identificar las causas de incumplimiento.

II. Implementar acciones correctivas.

III. Revisar las acciones correctivas para verificar la eficacia e identificar deficiencias o debilidades.

IV. Registrar y mantener evidencia de los controles.