POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

SEGURIDAD DE LA INFORMACIÓN

Red de Universidades Anáhuac

CONTENIDO

INTRODUCCIÓN

La Red de Universidades Anáhuac tomó la decisión como parte de su planeación estratégica, de implantar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001:2022, con el objetivo de asegurar el cumplimiento de los requisitos de información de las partes interesadas, contractuales, legales, normativas y cualquier otro requisito aplicable a las operaciones del negocio.

La base del Sistema de Gestión de Seguridad de la Información de la RUA es el mantenimiento y mejora de procesos que gestionan eficientemente la Seguridad de la Información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información y minimizando los riesgos de Seguridad de la Información de la RUA.

Misión

“Contribuir a la formación integral de líderes de acción positiva y promover institucionalmente el desarrollo de las personas y de la sociedad, inspirados en los valores del humanismo cristiano.”

Visión 2024

“Ser referente de un modelo académico de vanguardia internacional, así como, una experiencia trascendente y significativa, que apoye el desarrollo de las personas, para que sean agentes de liderazgo y de transformación, consolidando el crecimiento del campus y capitalizando la red de egresados para establecer mayor vinculación con los sectores estratégicos.”

OBJETIVO DE LA POLÍTICA

Esta Política establece los principios y directrices para proteger la información de la Institución y es creada, autorizada y difundida por la Alta Dirección que se encuentra conformada por la DTI de SERUA, Secretario Técnico de la RUA y los miembros de la Junta de Dirección.

ALCANCE DEL DOCUMENTO

Esta Política es de carácter OBLIGATORIO, para todos los usuarios de la RUA, así como para los que requieran la utilización de la información y sistemas que la soportan.

Esta Política debe ser comunicada a todos los usuarios internos y, externos que procesen información de la RUA.

Esta Política podrá incluir procedimientos, manuales, lineamientos u otros documentos necesarios para su adecuado desarrollo e implementación, en caso de ser requerido.

RESPONSABILIDADES

Todos los colaboradores y/o usuarios de la Red de Universidades Anáhuac, son responsables de acatar estas políticas bajo los siguientes roles y responsabilidades:

Alta Dirección	Conformada por la DTI de SERUA, Secretario Técnico de la RUA y los miembros de la Junta de Dirección, quienes dan apoyo y autorización al Sistema de Gestión de Seguridad de la Información (SGSI), con el fin de que todos los colaboradores y usuarios se comprometan con la ejecución de las políticas establecidas.
Comité de Ciberseguridad	El Comité de Ciberseguridad está conformado por representantes de las áreas de Tecnología de la información de la RUA y son responsables de la revisión y autorización de esta política.
Comunidad Anáhuac	Empleados, profesores, alumnos, prospectos, padres de familia o tutores, proveedores.
Responsable general del SGSI de la RUA	Es el responsable del SGSI y responsable de la revisión, actualización y divulgación de este documento.

Responsable Local del SGSI	Son los responsables del SGSI en cada Universidad, responsables del entendimiento de esta política, su divulgación y sensibilización al interior de su Universidad.
Propietario o dueño de la información	Son los responsables de uno o varios activos de información y por lo tanto de identificar el nivel de seguridad que deben tener los activos de información a su cargo y comunicarlo a los responsables locales del SGSI. También son responsables de acatar esta política y verificar su cumplimiento sobre los activos a su cargo.
Usuario	Son todas las personas que han sido autorizadas para utilizar los sistemas, aplicaciones o activos de información de la RUA, o bien que participan en un proceso de negocio, pueden ser internos o externos. También son responsables de seguir de manera estricta lo que indica esta política.

PROCESO DISCIPLINARIO O INCUMPLIMIENTO A ESTA POLÍTICA

Todos los usuarios internos y externos de la Red de Universidades Anáhuac, que accedan, procesen y/o almacenen información interna o de nuestros estudiantes, deben apegarse a esta Política de Seguridad de la Información.

El no apego a esta Política puede resultar en medidas disciplinarias que serán revisadas con el Comité de Ciberseguridad, el área de Capital Humano y el área Legal si fuera necesario, para evaluar la sanción pertinente, de acuerdo con el documento RUA-PRO-SGSI-04-Proceso disciplinario de seguridad de la información y ciberseguridad.

TÍTULO DE DOCUMENTO
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CÓDIGO	RUA-POL-SGSI-01

ELABORÓ	REVISÓ
Nombre Completo, Puesto y Firma	*Nombre Completo, Puesto y Firma*

AUTORIZÓ

Nombre Completo, Puesto y Firma

FECHA DE CREACIÓN	*dd/mm/aa*	**N° DE VERSIÓN**	**1**
FECHA DE ÚLTIMA ACTUALIZACIÓN	*dd/mm/aa*	**PERSONA Y PUESTO QUE REALIZÓ LA ÚLTIMA ACTUALIZACIÓN**	

GLOSARIO

Lista en orden alfabético de las palabras o expresiones que pudieran ser difíciles de comprender, junto con su significado o algún comentario

Término	Descripción
Activos de la información	Todo aquello relacionado con la información que tiene algún valor para la RUA; información, sistemas de información, bases de datos,

Término	Descripción
	servidores, equipos de cómputo, memorias, discos duros, servicios, personas, sus competencias, habilidades y experiencia que permiten que la información sea utilizada en los procesos de negocio de la RUA. Los activos de información pueden ser tangibles, como documentos físicos, o intangibles, como conocimientos y experiencia.
Aplicación	Programa informático diseñado como una herramienta para realizar operaciones o funciones específicas.
Código malicioso	Es un tipo de código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos
Comunidad Anáhuac	La comunidad Anáhuac está conformada por; Empleados, Maestros, Alumnos, Prospectos, Padres o tutores y Proveedores.
Confidencialidad	La información no se pone a disposición ni se revela a personas, entidades o procesos no autorizados.
Datos personales	Cualquier información concerniente a una persona física identificada o identificable.
Disponibilidad	Es asegurar que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.
Evento	Ocurrencia o cambio de un conjunto particular de circunstancias que pudieran llegar a afectar la Seguridad de la Información.
Incidente de Seguridad de la Información	Un evento o una serie de eventos de Seguridad de la Información no deseados o inesperados que tienen una probabilidad significativa de

Término	Descripción
	comprometer las operaciones y amenazar la Seguridad de la Información.
Integridad	Es asegurar que la información y sus métodos de proceso son exactos y completos.
Partes interesadas	Se refiere a personas u organizaciones que pueden afectar, verse afectadas o percibirse como afectadas por una decisión o actividad de la Institución. Las partes interesadas se pueden encontrar tanto fuera como dentro de la Institución y pueden tener necesidades, expectativas y requisitos específicos para la Seguridad de la Información de la Institución.
SI	Abreviatura de Seguridad de la Información.
Seguridad de la Información	La Seguridad de la Información es el conjunto de medidas que permite proteger los activos de información de la Red de Universidades Anáhuac y se basa en preservar su Confidencialidad, Integridad y Disponibilidad.
SGSI	Abreviatura de Sistema de Gestión de Seguridad de la Información.
Sistema de Gestión de Seguridad de la Información	Es un conjunto de políticas, procedimientos y directrices de seguridad de la información, que son administrados por la RUA.
Sistemas de información	Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información.
Software	Un conjunto de instrucciones, procedimientos, reglas y datos que, cuando se ejecuta en un sistema informático, proporciona la capacidad de realizar una tarea o función específica.
RUA	Abreviatura de Red de Universidades Anáhuac.
Virus	Programa o código malicioso escrito para modificar el funcionamiento de un equipo.

Marco Normativo	Reglamentos, acuerdos en los que se está basando. • ISO 27001:2022 Information security, cybersecurity and privacy protection — information security management systems — Requirements • ISO 27002:2022 Information security, cybersecurity and privacy protection — Information security controls • RUA-DOC-SGSI-03-Roles y responsabilidades de SGSI • RUA-POL-SGSI-04-Política de Clasificación de la Información • RUA-PRO-SGSI-03 Política de Accesos • RUA-PRO-SGSI-02 Procedimiento para la Gestión de Activos • RUA-PRO-SGSI-04-Proceso disciplinario de seguridad de la información y ciberseguridad • RUA-POL-SGSI-10 Política de seguridad para el desarrollo de software • RUA-PRO-SGSI-05-Gestión de Cambios

Anexos	Este documento no contiene anexos.

Control de cambios	Descripción del cambio y motivos de este (última actualización). Cada cambio que se agregue deberá guardarse en una versión nueva del Manual.			
	Versión	**Descripción y Motivo**	**Autor**	**Fecha**
	01	Versión original	*Nombre ComplMoeto*	*dd/mm/aa*

POLÍTICA DEL SGSI DE LA RUA

Para la Red de Universidades Anáhuac (en adelante RUA), es de gran importancia la protección de la información de nuestra Comunidad Anáhuac. Es por esto, que a través del Comité de Ciberseguridad conformado por una representación de la comunidad Anáhuac, se ha establecido

y autorizado la Política del SGSI, que se encuentra alineada a los requisitos del Sistema de Gestión de Seguridad de la Información (en adelante SGSI) y alineada al estándar de ISO 27001:2022.

El Comité de Ciberseguridad se compromete a analizar y gestionar los requisitos relacionados con la Seguridad de la Información y apoyar la mejora continua del SGSI, impulsando el cumplimiento de los siguientes objetivos:

- Determinar y alcanzar los niveles de seguridad que garanticen una adecuada protección de la información y de la plataforma tecnológica en que se procesa, transmite y almacena.
- Proteger los activos de información de la destrucción, la indisponibilidad, la manipulación o la divulgación no autorizada para su adecuado mantenimiento en un entorno seguro.
- Promover y fomentar una conciencia de Seguridad de la Información, como una estrategia para el cumplimiento de los objetivos de la RUA.
- Vigilar el cumplimiento de los requisitos y procesos de los servicios de TI.
- Cumplir con las leyes y regulaciones vigentes en materia de seguridad y protección de la información.

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La Seguridad de la Información es el conjunto de medidas que permite proteger los activos de información de la Red de Universidades Anáhuac y se basa en preservar su Confidencialidad, Integridad y Disponibilidad.

Los principios de Seguridad de la Información guían las acciones para alcanzar niveles adecuados en confidencialidad, integridad y disponibilidad de la información, los principios que en la RUA queremos alcanzar a través de esta Política son:

- Protección de la información en el uso, divulgación, copia, modificación, manipulación y destrucción no autorizados.
- Protección de la información de acuerdo con su valor, importancia y confidencialidad.
- Consistencia de la información y sus accesos, de acuerdo con las Políticas y normativas implementadas.
- Protección de la información, de acuerdo con su clasificación, ver documento RUA-POL-SGSI-04 Política de Clasificación de la Información.
- La información generada, documentada, impresa, hablada o almacenada en sistemas electrónicos, manejada por y en nombre de la Universidad Anáhuac, se considera como propia de esta; la provista de manera confidencial por terceros es propiedad de estos.
- Los Datos Personales son propiedad de cada uno de sus titulares.

- Los usuarios deben participar activamente en la capacitación y concienciación que se proporcione en materia de Seguridad de la Información.
- Todo acceso, uso y gestión de la información deberá cumplir con sus políticas y normas.
- La RUA tiene el compromiso de establecer, mantener y mejorar los controles necesarios para el cumplimiento de leyes y regulaciones que resulten aplicables en materia de Seguridad de la Información.

Uso correcto de activos de información

El uso correcto de los activos de información involucra una serie de actividades que permite su uso adecuado y la Seguridad de la Información, por lo que deben ser protegidos ante amenazas internas y/o externas como se indica a continuación:

- Proteger contra pérdida, mal uso, robo o modificación no autorizada.
- Tener un propietario o dueño que se encargue de supervisar el activo de información y su buen funcionamiento.
- Mantener la integridad, disponibilidad y confidencialidad de los activos de información.
- Utilizar sólo los activos de información autorizados. Los recursos informáticos autorizados y/o distribuidos, tales como correo electrónico, Internet, equipos informáticos, teléfonos móviles, etc., sólo podrán ser utilizados para fines relacionados a sus funciones laborales y deberán contar con un método de bloqueo como contraseñas y con bloqueo de pantalla después de pasar un tiempo de inactividad, así como, MFA y la utilización de biométricos en caso de que la plataforma o tecnología lo permita.
- Comprar hardware y software sólo a través del área correspondiente de TI.
- Clasificar y etiquetar la información de acuerdo como lo estipula el documento RUA-POL-SGSI-04 Política de Clasificación de la Información.
- Evitar beber líquidos y comer alimentos junto a computadoras o archivos de trabajo.
- Cuidar y asegurar los dispositivos electrónicos portátiles que almacenen información, tales como; computadoras portátiles y teléfonos móviles.
- No dejar desatendidos equipos y medios de almacenamiento fuera de las instalaciones en lugares públicos y no seguros.
- Evitar el uso de dispositivos móviles de la empresa en lugares que no brinden la seguridad física necesaria para evitar pérdidas o robos.

Uso incorrecto de los activos de información

Cuando se tiene un uso incorrecto de los activos de información, se pone en riesgo la Seguridad de la Información de los colaboradores y de los estudiantes, motivo por el cual es de suma importancia cuidar NO realizar ninguna de las siguientes actividades:

- Abrir correo electrónicos o enlaces de internet que no sean confiables.
- Utilizar los recursos informáticos para acceder, almacenar o distribuir contenidos que se consideren ilegales, inapropiados u ofensivos.
- Usar software sin licencia en cualquier equipo institucional. Esto también incluye violar los términos y acuerdos de cualquier producto de software con licencia.
- Instalar software no autorizado por el área de TI.
- Intentar o eludir con éxito los controles de seguridad del sistema o ver, alterar o destruir datos, software o hardware sin autorización.
- Utilizar la cuenta, contraseña o sesión de computadora de otro usuario, ya sea por suplantación de identidad o por que el titular haya compartido sus credenciales.
- Usar de forma no autorizada las contraseñas de bases de datos, servidores y sistemas.
- Las cuentas de correo institucionales no deben ser usadas con propósitos particulares personales.
- Eliminar o destruir de forma no autorizada el hardware, software o la información.
- El acceso a información confidencial sin autorización.
- Violaciones de leyes y reglamentos estatales, federales o internacionales.
- Almacenar información propiedad de la RUA o de estudiantes en equipos de cómputo personales.
- Tomar fotos o videos de computadoras, infraestructura, tecnología o de las áreas que tengan infraestructura tecnológica.

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información busca la adopción de un conjunto de medidas que nos ayudan a preservar la confidencialidad, integridad y disponibilidad de la información y tiene como objetivo proteger la información, los activos de información y dar seguimiento y cumplimiento al Sistema de Gestión de Seguridad de la Información (SGSI).

A través del SGSI buscamos contar con medidas de protección que nos ayuden a dar frente a amenazas de seguridad que pueden presentarse sobre nuestros activos.

Todos los colaboradores de la RUA cubrimos uno o más roles dentro del SGSI, motivo por el cual es importante identificar nuestro rol y las políticas que debemos cumplir, como se indica en el apartado de responsabilidades de este documento.

Política de uso de dispositivos móviles

Se proveerá de dispositivos móviles a los usuarios que así lo requieran para el desempeño de sus funciones, previa revisión y autorización por responsable de área y responsables de la autorización de compra de equipos. Como dispositivos móviles se incluyen laptops, celulares, tabletas y medios de almacenamiento extraíbles como discos duros, USB, entre otros. Para el uso adecuado y seguro de estos dispositivos se deberán seguir las siguientes políticas:

- Establecer un método de bloqueo como contraseña y/o doble factor de autenticación (cuando la aplicación lo permita).
- Configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.
- No modificar las configuraciones de seguridad de los dispositivos móviles bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Evitar la instalación de programas, desde fuentes desconocidas; se deben instalar sólo aplicaciones autorizadas.
- Aceptar las actualizaciones de los dispositivos móviles.
- Evitar hacer uso de redes inalámbricas de uso público.
- Desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos, cuando no sean requeridas.
- Evitar conectar los dispositivos móviles asignados, por puerto USB, a cualquier dispositivo desconocido, de uso compartido, de hoteles o cafés internet, entre otros.
- No almacenar vídeos, fotografías o información personal en los dispositivos móviles asignados.

Política de acceso a la información

El acceso a los activos de información debe otorgarse cuando los usuarios estén autorizados de acuerdo con las funciones que desempeñan y se debe cumplir con el principio de mínimo privilegio o acceso mínimo requerido y de acuerdo con las siguientes políticas:

- Los usuarios solo deben tener acceso a la información y otros activos asociados que sean necesarios para realizar sus funciones laborales.

- Se debe tomar en cuenta la clasificación de la información para proporcionar accesos y privilegios.
- Los accesos no deben estar asociados a cuentas de correo electrónico personales, sólo a cuentas de correo electrónico institucionales.
- Los accesos deben removerse cada que existan bajas o cambios de puesto y los privilegios deben revisarse cada que exista un cambio de función o puesto.
- Ejecutar los accesos de usuarios de acuerdo con un proceso formal de altas y bajas de usuarios para la asignación de derechos de acceso.
- Los usuarios son responsables de todas las actividades que ocurran bajo su cuenta de acceso a los activos de información.
- Solo los administradores autorizados pueden otorgar privilegios a los usuarios para acceder a las redes, directorios, archivos o aplicaciones.
- Los derechos y privilegios de administrador (usuarios privilegiados) se otorgan sólo a aquellos usuarios, como administradores de sistemas, redes, dominios o aplicaciones.
- Los usuarios internos y externos sólo deben tener acceso a la red y a los servicios de red a los que han sido específicamente autorizados.

Política sobre el uso de contraseñas

Los usuarios asignados a cada activo de información deben contar con una contraseña robusta, esto es, con las características de seguridad necesarias que garanticen que el acceso a la información es seguro y sólo puedan acceder las personas autorizadas y con los privilegios necesarios para el tratamiento de la información, las políticas a seguir para el uso de contraseñas son:

- Todo identificador de usuario (ID) y contraseña debe ser informado al solicitante de manera segura y nunca en un mismo medio de notificación, como canales de comunicación Institucionales.
- Los usuarios deberán cambiar las contraseñas temporales, de manera inmediata después de ser asignadas.
- El identificador de usuario (ID) y contraseña no deben ser dados a conocer a otras personas.
- La creación de las contraseñas no se basa en nada que otra persona pueda adivinar u obtener fácilmente, no en palabras del diccionario o combinaciones de estas.
- Al generar una nueva contraseña evitar reutilizar una de las últimas cinco contraseñas anteriores creadas en el mismo sistema.
- Las contraseñas deben ser cambiadas cada 90 días, aun cuando el sistema no solicite el cambio automáticamente.

- En caso de sospechar que una contraseña sea comprometida o es conocida por alguien no autorizado, se debe cambiar inmediatamente y reportar al Responsable Local del SGSI.
- Las mismas contraseñas no pueden ser utilizadas en distintos servicios y sistemas.
- Para la creación de las contraseñas se debe considerar lo siguiente:
    - Contar con una longitud mínima de 8 caracteres
    - Para usuarios privilegiados, que son aquellos con acceso a; servidores, bases de datos o que tienen privilegios de administrador, deberán contar con una longitud mínima de 12 caracteres.
    - Las contraseñas deben estar compuestas por lo menos con; un carácter en mayúsculas, un número y un carácter especial (#@/&%).
    - Se recomienda utilizar la técnica "passphrase", que se define por utilizar una cadena de palabras similar a una oración, en donde una colección de palabras comunes se puede utilizar al azar y en donde algunos caracteres se pueden cambiar por caracteres especiales, ejemplo:
        - ArbolVerde = @rb0!V3rd3
        - CiudadAlegre = C!u6a6@L3gr3
        - Nota: No utilizar estos ejemplos.
- En caso de que la aplicación no permita esta configuración de contraseña, se debe adecuar al requerimiento del aplicativo.
- Las contraseñas están consideradas como información confidencial, por lo cual, es importante no compartirlas, no escribirlas en libretas o post-it, ni dejarlas a la vista.
- Es importante activar el doble factor de autenticación en las herramientas y/o aplicaciones que lo soporten y que serán sugeridas por el área de TI.
- El doble factor de autenticación o verificación en dos pasos es un método seguro para probar la identidad del usuario y agrega un nivel adicional de seguridad.
- La primera opción es agregar una contraseña y la segunda es a través de un medio como un mensaje SMS indicando un código de seguridad que debe ser ingresado por el usuario.
- Si el sistema o aplicación se bloquea por varios intentos erróneos al ingresar la contraseña o por no cambiarla a tiempo, se debe solicitar al equipo de TI o propietario del sistema su desbloqueo.
- En caso de requerir renovación de una contraseña, solicitar al área de TI.
- Si los sistemas no permiten el cambio de contraseña, solicitar al equipo de TI la generación de una nueva contraseña apegada a los lineamientos aquí establecidos.

Política sobre la transferencia de la información

La información debe ser transferida de forma segura, utilizando métodos que protejan su confidencialidad, integridad y disponibilidad. La transferencia de información se refiere al envío y recepción de información a través de aplicaciones o de dispositivos electrónicos y se deberán cumplir las siguientes políticas para su uso:

- La transferencia de información electrónica sólo podrá ser a través de aplicaciones o software autorizado.
- Para transferir documentación física o activos de información físicos clasificados como confidencial utilizar servicios de mensajería y transportes confiables ver el documento RUA-POL-SGSI-04 Política de Clasificación de la Información.
- El envío de información a través de correo electrónico debe ser utilizando la cuenta institucional.
- Toda información confidencial enviada por correo electrónico deberá contar con una contraseña segura.
- Para el envío de correos electrónico siempre se debe confirmar la dirección del destinatario para validar que información confidencial no llegue a manos de personas no deseadas.
- Los archivos anexos en correos electrónicos deben ser revisados con un antivirus antes de ser abiertos.
- No se debe enviar información laboral, interna o de estudiantes a través de correos electrónicos personales.
- Los procedimientos de intercambio de información con personal externo deben apegarse a lo estipulado en los contratos o bases del proyecto correspondiente.
- Las aplicaciones gratuitas de mensajería instantánea no son herramientas institucionales y por lo tanto no podemos garantizar la seguridad en la transferencia de información, su uso debe ser bajo supervisión de los responsables de cada área. y previa aprobación por parte del área de TI para uso institucional.
- No se puede transferir información clasificada como confidencial a través de aplicaciones gratuitas de mensajería instantánea.

Política sobre escritorio y pantalla despejada

Para mantener la seguridad y evitar la exposición de información en los lugares de trabajo, es importante cumplir las siguientes políticas:

- Evitar ingerir alimentos o bebidas cerca de dispositivos móviles, equipos de cómputo y documentos físicos, así como, evitar manipular líquidos en su cercanía.
- Bloquear la sesión de usuario, cuando se ausente del área o puesto de trabajo y/o deje los equipos desatendidos, para proteger el acceso a la información.
- Evitar colocar accesos directos en el desktop o pantalla de la computadora.
- Cerrar correctamente la sesión de usuario y apagar el equipo de cómputo y periféricos, cuando finalice la jornada laboral, garantizando con esto, una desconexión satisfactoria de la red y sistemas.

- Evitar dejar notas con datos sensibles como: nombre de usuario, contraseñas de acceso, números de cuenta o teléfonos personales.
- Guardar bajo llave documentos físicos y dispositivos móviles en cajones, archiveros o sitios seguros, una vez que se dejó de utilizar y cuando se ausente del puesto de trabajo.
- Si por funciones del puesto se maneja información confidencial y se dispone de un área de oficina independiente, deberá cerrar con llave si se ausenta físicamente del área.
- Retirar la información sensible de rotafolios, pizarras y otros equipos utilizados para presentaciones de información una vez concluida las sesiones de trabajo.
- Retirar de las impresoras y escáneres toda documentación física, incluyendo la que se encuentre desatendida.

Política sobre trabajo remoto

Cuando se realice trabajo remoto previamente autorizado por los responsables de área, debe realizarse siguiendo las medidas de seguridad establecidas para proteger la información accedida, procesada o almacenada.

- Las conexiones remotas hacia los recursos tecnológicos de la RUA, deben contar con las aprobaciones requeridas y acatar las condiciones de uso establecidas.
- Utilizar conexiones seguras y tratar de evitar utilizar dispositivos públicos, de hoteles o cafés internet, entre otros.
- En caso de usar conexiones públicas, al inicio de la conexión deberá de hacer uso de VPN para hacer uso de los mecanismos de seguridad instrumentados en la red de su Universidad.
- Bloquear las sesiones de los equipos de cómputo y dispositivos móviles cuando no se estén utilizando para proteger la información, aun estando en casa.
- Resguardar los documentos físicos de trabajo cuando no sean utilizados para que no estén a la vista ni sufran algún percance.
- Apagar diariamente los equipos de cómputo con el fin de que se corran las actualizaciones del equipo y no queden expuestos ante virus o ataques maliciosos y mantener activos los mecanismos de búsqueda automática de actualizaciones que dispongan los diferentes proveedores de software.

Política para la seguridad de activos fuera de las instalaciones

Cuando los activos de información requieran ser retirados fuera de las instalaciones, se deberán seguir los siguientes lineamientos:

- Seguir las instrucciones del fabricante para la protección de los equipos, por ejemplo; exposición a campos electromagnéticos fuertes, agua, calor, humedad o polvo.
- No dejar desatendidos equipos o medios de almacenamiento en lugares públicos y no seguros.
- Proteger la visualización de la información en lugares público.
- Cuando el equipo es transferido por un proveedor o tercero, mantener un registro que defina la cadena de custodia y especificar la organización que se hace responsable del equipo. La información que no necesita transferirse con el equipo debe eliminarse de forma segura.

Política para el Desarrollo de sistemas, software o aplicaciones

- Los usuarios que por necesidad de su operación requieran de un nuevo desarrollo, deberán registrarlo como un proyecto, ver documento RUA-DOC-SGSI-08-Seguridad Información en Proyectos.
- Los desarrollos realizados por la RUA deberán cumplir con la política RUA-POL-SGSI-10 Política de seguridad para el desarrollo de software.
- Los desarrollos subcontratados con terceros también deben apegarse a la política RUA-POL-SGSI-10 Política de seguridad para el desarrollo de software, y obtener el visto bueno por parte del área de TI para su implementación en la Institución y verificar su compatibilidad con la tecnología existente.
- Todos los cambios al software e infraestructura existente, deberá pasar por el proceso de cambios existente, ver documento RUA-PRO-SGSI-05-Gestión de Cambios.

Política para el reporte de incidentes de Seguridad de la Información

Un incidente de Seguridad de la Información es cualquier evento que pueda comprometer la confidencialidad, integridad o disponibilidad de la información de la Institución.

Todos los usuarios deben ser conscientes de su responsabilidad para informar los incidentes de Seguridad de la Información que detecten, para prevenir o minimizar el efecto que estos puedan tener sobre los activos de información.

Los usuarios notificarán sobre una sospecha de incidente de Seguridad de la Información por medio de la Herramienta de Gestión de Servicios. Esta herramienta contará con la clasificación del incidente para su selección, como se indica a continuación:

- Ataques Físicos.

- Daño no intencional o accidental, pérdida de información o pérdida de activos.
- Incidentes por desastres naturales o ambientales.
- Incidentes por fallas o mal funcionamiento.
- Incidentes por la interrupción o falta de insumos.
- Incidentes por intercepción de información.
- Incidentes por actividad maliciosa con el fin de tomar el control, desestabilizar o dañar un sistema informático.
- Incidentes que afectan a políticas, normativas y regulaciones

Posterior a la selección con base a las anteriores definiciones, los usuarios agregarán una breve descripción del incidente para su mayor entendimiento y análisis.

Generales

Cada responsable de área verificará que el personal bajo su responsabilidad cumpla con las Políticas de Seguridad de la Información aquí descritas, en caso de encontrarse un incumplimiento, se debe reportar al Responsable local del SGSI para dar seguimiento de acuerdo con el documento RUA-PRO-SGSI-04-Proceso disciplinario de seguridad de la información y ciberseguridad, para identificar las causas y evaluar las acciones correctivas.

Este documento será revisado y, de ser necesario, actualizado una vez al año por el dueño del documento.

Este documento se complementa con las normativas generadas para el SGSI.