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

# POLÍTICA DE SEGURIDAD PARA PERSONAL VISITANTE O EXTERNO

Última Fecha de Actualización: Junio 27, 2022



SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
Matamoros SN, Zona Centro
Ciudad Victoria, Tamaulipas,
C.P. 87000

(834) 318-1800, ext. 2823
www.uat.edu.mx

CONTROL DE VERSIONES

| Datos del Documento | |
|---|---|
| Aplicado a | Direcciones del alcance del Sistema de Gestión de la Seguridad de la Información (SGSI) |
| Aprobado por | Directores del SGSI |
| Fecha de Aprobación | 27/06/2022 |
| Fecha de Revisión: | 27/06/2022 |
| Versión | 4.0 |
| Clasificación | Público |
| **Cambios desde la última versión**<br>Se modifica la tabla de control de versiones. | |

TABLA DE CONTENIDOS

SECCIÓN I
ASPECTOS GENERALES

1.1 Objetivo general

Limitar el acceso a la información y a las instalaciones de procesamiento de la información para proteger la confidencialidad, integridad y disponibilidad de la información y sistemas manejados por la Universidad

1.2 Alcance

Esta política aplica a los visitantes externos que tengan acceso a la información de la Universidad e intercambien, procesen, almacenen, modifiquen, o utilicen sus equipos de cómputo en la red, que hagan uso de la infraestructura, plataformas tecnológicas y los sistemas de información, equipos portátiles, dispositivos móviles propiedad de la Universidad o creen nueva información confidencial propiedad de la Universidad

1.3 Definiciones, siglas y acrónimos

- **Activos de TI:** Aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos y archivos electrónicos y la información contenida en éstos.
- **Colaboradores:** Personal que mantiene una relación laborar con la Universidad Autónoma de Tamaulipas dentro de los siguientes esquemas: estructura, por honorarios y tercerización (outsourcing).
- **Equipo de escritorio:** Es un tipo de computadora personal, diseñada y fabricada en una ubicación fija, como un escritorio o mesa de trabajo.
- **Equipo portátil:** Es un tipo de computadora que integra todos los elementos necesarios para un correcto funcionamiento, dispuesto en una carcasa pequeña y de fácil transportación.
- **Imagen ISO:** Tipo de archivos en donde se guardan todos los datos de un CD, un DVD, un Disco Duro, etc. Para hacer una copia de seguridad, para clonarlos o facilitar su transporte, etc. Se guardan en formatos con ISO, BIN, etc.
- **LFPDPPP:** Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- **LPI:** Ley de la Propiedad Industrial.
- **Lugar de trabajo:** Es cualquier lugar físico o virtual donde uno o más usuarios desarrollan sus tareas.
- **Lugar seguro:** Es aquel que protege los activos de TI de accesos no autorizados, por ejemplo: caja fuerte, cajones bajo llave, oficinas con llave, etc.
- **Medios de almacenamiento:** Son elementos técnicos destinados a proveer de espacio físico para albergar archivos.


Matamoros SN, Zona Centro
Ciudad Victoria, Tamaulipas,
C.P. 87000
(834) 318-1800, ext. 2823
www.uat.edu.mx

- **Teletrabajo:** Se refiere a todas las formas de trabajo fuera de la oficina, incluyendo entornos de trabajo no tradicionales, tales como los denominados "trabajos remotos", "lugar de trabajo flexible"," trabajo a distancia" y entornos "virtuales de trabajo".
- **SGSI:** Sistema de Gestión de la Seguridad de la Información.
- **Universidad:** Universidad Autónoma de Tamaulipas.
- 
- **SST:** Secretaría de Salud de Tamaulipas.


Matamoros SN, Zona Centro
Ciudad Victoria, Tamaulipas,
C.P. 87000
(834) 318-1800, ext. 2823
www.uat.edu.mx

SECCIÓN II
POLÍTICA

2.1 Cumplimiento

- NMX-I-27001-NYCE-2015 / Apéndice A / A.5.1.1 Políticas para la Seguridad de la Información.
- NMX-I-27001-NYCE-2015 / Apéndice A / A.7.1.2 Términos y condiciones de la relación laboral.
- NMX-I-27001-NYCE-2015 / Apéndice A / A.9.1.1 Política de control de acceso.
- NMX-I-27001-NYCE-2015 / Apéndice A / A.15.1.1 Política de Seguridad de la Información para la Relación con Proveedores.
- NMX-I-27001-NYCE-2015 / Apéndice A / A.15.1.2 Abordar la seguridad dentro de los acuerdos del proveedor

2.2 Política de Seguridad para Personal Visitante o Externo

**2.2.1 Generales**

- Revisar la Solicitud de entrada y salida de equipo de proveedores o personal externo autorizado para el ingreso a las instalaciones de la persona visitante.

- Cuando se registre periodos de contingencia sanitaria, respetar las medidas de seguridad establecidas en los accesos del edificio y cumplir con las medidas de sanidad en base a los lineamientos establecidos por la SST: Como uso de tapete sanitizante, aplicar gel antibacterial, uso de cubrebocas, sana distancia, entre otras.

- Registrar en la Bitácora de entrada y salida de externos y equipo, los siguientes datos de: Fecha y hora de ingreso. Fecha y hora de salida, Nombre de la persona que visita, y en la Bitácora de equipo de visitante Fecha y hora de ingreso. Fecha y hora de salida, tipo de activo, características número de serie, de los equipos del visitante que ingresarán a las instalaciones.

- Otorgar el acceso siempre y cuando la persona que visita de su autorización.

- Solicitar una identificación y revisar que el personal externo porte un gafete que lo identifique como tal durante su estancia en las instalaciones. En caso de contingencia y para cumplir con las medidas sanitarias, solo se registrará el acceso del visitante.

- Los proveedores sólo podrán desarrollar para la Universidad aquellas actividades establecidas en el contrato de prestación del servicio u otro equivalente.

- Los proveedores deberán proteger la confidencialidad, integridad y disponibilidad de la información propiedad de la Universidad, tal y como lo establece el contrato de confidencialidad

- Los proveedores que presten el servicio de desarrollo de Software a la Universidad deben implementar normas o las mejores prácticas de la industria en el desarrollo de las aplicaciones para garantizar la seguridad de los sistemas.

- El proveedor controlará la salida de información propiedad de la universidad. que se encuentre alojada bajo los dispositivos que administra y controla, estos controles deberán ser notificados a la universidad por el tiempo de duración de la relación contractual.

- Informar a la Universidad cualquier fuga, pérdida o alteración de información y la correspondiente medida de mitigación.

- El proveedor responde directamente por el acceso que sus empleados tengan a documentos confidenciales de la Universidad y deberá entenderse que este acceso es estrictamente temporal, sin otorgarle derecho alguno de titularidad o copia sobre dicha información.

- El proveedor que preste el servicio de alojamiento u otro servicio en la nube a la Universidad deberá realizar pruebas de penetración internas y externas sobre la infraestructura y aplicaciones, así como análisis de vulnerabilidades sobre los servidores y dispositivos de red internos y externos; las cuales deberán efectuarse por personal calificado y según los estándares de la industria. Cada vez que se lleve a cabo esta actividad, deberá presentar un informe con los resultados a la Universidad.

### 2.2.2 Acceso a Instalaciones críticas

- Contar con autorización del responsable de la infraestructura tecnológica, que atienda al visitante en áreas críticas como el Centro de Datos Principal.

- Vigilar siempre al proveedor externo durante su estancia en las instalaciones críticas por parte del responsable de la infraestructura tecnológica.

- Evitar el uso de equipo tecnológico, de grabación o video dentro de las instalaciones críticas.

### 2.2.3 Acceso a la Información

- Firma de un convenio de confidencialidad y acuerdo de transferencia de la información por parte del proveedor.
- Solicitar y contar con una autorización formal por el director del área para el acceso del proveedor a área criticas como el Centro de Datos Principal, donde se indique el motivo del envío de información, documentación que se enviará, medio utilizado para él envió y periodo autorizado.
- Cumplir con las medidas y protocolos de seguridad técnicas para la transferencia de la información.
- Retirar el acceso otorgado cuando la seguridad de la información se vea comprometida o al finalizar el periodo autorizado.

### 2.2.4 Uso de los Recursos de la universidad

La universidad debe comunicar las siguientes políticas al personal visitante por algún medio:

- No dañar física o lógicamente los equipos o la infraestructura tecnológica.
- No tomar fotografías sin previa autorización.
- No utilizar los recursos de la universidad sin previa autorización.
- Evitar la descarga de programas, fotos, música, videos que no estén justificados durante su visita utilizando recursos de la universidad.
- No conectar, desconectar, desmantelar, retirar o cambiar partes, reubicar equipos o cambiar de configuración a los mismos sin autorización.
- No Instalar dispositivos de comunicaciones en los equipos e infraestructura tecnológica proporcionados por nombre de la organización.
- No realizar acciones o actividades que incumplan regulaciones de seguridad de la información o la normatividad aplicable.

2.3 Consecuencias y sanciones

La violación por acción y omisión de esta política de seguridad de la información de la Universidad implica, actualiza y/o genera sanciones en término de la normatividad aplicable. La supervisión de la adecuada aplicación de esta política estará a cargo de los órganos de vigilancia de la Universidad.

2.4 Documentos relacionados

- Código de Ética y Conducta de la Universidad Autónoma de Tamaulipas.
- Ley de la Propiedad Industrial.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tamaulipas.
- Ley de Transparencia y Acceso a la Información Pública del Estado de Tamaulipas.
- Ley Federal del Derecho de Autor.
- Ley General de Contabilidad Gubernamental.
- Norma Oficial Mexicana NOM-002-STPS-2010, Condiciones de seguridad-Prevención contra incendios en los centros de trabajo.
- Norma Oficial Mexicana NOM-003-SEGOB/2011, Señales y Avisos para Protección Civil.
- Norma Oficial Mexicana NOM-026-STPS-2008, Colores y Señales de Seguridad e Higiene, Identificación de Riesgos por Fluidos en Tuberías.
- Reglamento de Adquisiciones.
- Reglamento de Control Patrimonial.
- Reglamento de Investigación.
- Reglamento de Obras y Servicios relacionados con las mismas.

- Reglamento de Seguridad de la Información.
- Reglamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales para la Universidad Autónoma de Tamaulipas.