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
RECOMENDACIONES EN EL USO DE DISPOSITIVOS MÓVILES

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	5.0
Clasificación	Público
Cambios desde la última versión Se modifica la tabla de control de versiones.	

TABLA DE CONTENIDOS

SECCIÓN I
ASPECTOS GENERALES

1.1 Objetivo General

Proteger el acceso, proceso o almacenamiento de la información en los dispositivos móviles (equipos portátiles, teléfonos celulares) contra posibles riesgos como: mal uso, robo, modificación, entre otros.

1.2 Alcance

Estas recomendaciones aplican a la comunidad universitaria, que hace uso de las tecnologías de la información por medio de dispositivos móviles personales y /o proporcionados por la universidad.

1.3 Definiciones, Siglas y Acrónimos

- **SGSI:** Sistema de Gestión de la Seguridad de la Información.
- **Universidad:** Universidad Autónoma de Tamaulipas.
- **USB:** Universal Serial Bus (Bus Universal en Serie, en castellano). Se trata de un concepto de la informática para nombrar al puerto que permite conectar dispositivos a un equipo de cómputo.
- **VPN:** Virtual Private network. También llamada red privada virtual, es un tipo de tecnología conectada a la red que permite seguridad en la red local cuando el dispositivo está conectado a internet.

SECCIÓN II
RECOMENDACIONES DE USO

2.1 Cumplimiento

- NMX-I-27001-NYCE-2015 / Apéndice A / A.6.2.1 Política de dispositivos móviles.

2.2 Recomendaciones de uso para Dispositivos Móviles

Se recomienda que cualquier dispositivo móvil personal y/o proporcionado por la Universidad que contenga información de la universidad, conozca las siguientes medidas de seguridad.

2.2.1 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.

2.2.2 Teléfono 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.

2.2.3 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.

2.3 Documentos Relacionados

- Reglamento de Seguridad de la Información.
- Portal de Instituto Federal de Telecomunicaciones. Consulta número IMEI (Identidad Internacional de Equipo Móvil) (http://www.ift.org.mx/usuarios-y-audiencias/consulta-de-imei).