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 TRANSFERENCIA DE LA INFORMACIÓN

Última Fecha de Actualización: agosto 30, 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	30/08/2022
Fecha de Revisión:	30/08/2022
Versión	2
Clasificación	Público
Cambios desde la última versión Se agrego el nombre de política a transferencia de información. Se agrego la política de controles criptográficos a documentos relacionados.	

TABLA DE CONTENIDO

SECCIÓN I 4
ASPECTOS GENERALES 4
1.1 Objetivo general 4
1.2 Alcance 4
1.3 Definiciones, siglas y acrónimos 4
SECCIÓN II 5
POLÍTICA 5
2.1 Cumplimiento 5
2.2 Política de Transferencia de la Información 5
2.3 Consecuencias y sanciones 6
2.4 Documentos relacionados 6

SECCIÓN I
ASPECTOS GENERALES

1.1 Objetivo general

Proteger la transferencia de la información a través de medios electrónicos contra incidentes y usos ilícitos y evitar ataques por esta vía.

1.2 Alcance

Esta política aplica a todo el personal de las áreas que gestiona tecnologías de la información en la Universidad, así como personal externo contratado para servicios tercerizados que hagan uso de la infraestructura de TI, plataformas tecnológicas y los sistemas de información de la Universidad.

1.3 Definiciones, siglas y acrónimos

- **Colaborador:** Personal que mantiene una relación laborar con la Universidad Autónoma de Tamaulipas dentro de los siguientes esquemas: estructura, por honorarios y tercerización (outsourcing).
- **Equipos portátiles:** Es un tipo de computadora que integra todos los elementos necesarios para un correcto funcionamiento, dispuestos en una carcasa pequeña y de fácil transportación.
- **Lugar de trabajo:** Es cualquier lugar físico o virtual donde uno o más usuarios desarrollan sus tareas.
- **Universidad:** Universidad Autónoma de Tamaulipas.

SECCIÓN II
POLÍTICA

2.1 Cumplimiento

- MX-I-27001-NYCE-2015 / Apéndice A / A.13.2 Transferencia de información

2.2 Política de Transferencia de la Información

Cualquier personal de las áreas que gestiona tecnologías de la información en la Universidad, así como personal externo contratado que requiera transferir información de manera electrónica debe tomar en cuenta las recomendaciones para la seguridad de 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

Generales

- Los medios de transferencia de información institucionales son los relacionados a la cuenta institucional: Correo electrónico de Microsoft Office 365, Microsoft Teams, One drive, Share point; y otros medios de comunicación como teléfono fijo o móvil y grupos redes sociales.
- Se recomienda la instalación y actualización periódica de soluciones de antispam y antivirus a nivel institucional en la plataforma de correo electrónico o zona perimetral.
- Se recomienda cifrar el correo electrónico y la protección con contraseña a los archivos adjuntos siguiendo las recomendaciones de la política de Controles Criptográficos y él envió de la contraseña en otro correo o medio de comunicación para proteger la información confidencial y asegurar la autenticidad de la empresa como remitente.
- Se recomienda utilizar solo el correo institucional para la transferencia de información propiedad de la universidad y evitar el envió de mensajes en cadena o información irrelevante para la universidad.
- Se recomienda retener y depurar la información compartida al término del plazo acordado
- Se recomienda no dejar mensajes que contienen información confidencial sobre los buzones de voz o cuentas de servicios, ya que pueden ser reproducidos por personas no autorizadas.
- Se recomienda concientizar al personal de no tener conversaciones confidenciales en lugares públicos o en canales de comunicación no seguros, oficinas abiertas y lugares de reunión.
- Se recomienda identificar y revisar regularmente los convenios de confidencialidad o acuerdos de no divulgación que reflejan las necesidades de protección de la información de la UAT

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 del órgano interno de control.

2.4 Documentos relacionados

- Recomendaciones en el uso de dispositivos móviles.
- Reglamento de seguridad de la Información.
- Política de control de acceso a las redes y los servicios de la red.
- Política de teletrabajo.
- Política de controles criptográficos.