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 SOFTWARE
Última Fecha de Actualización: junio 29, 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	Comité de Tecnologías de la Información
Fecha de Aprobación	29/06/2022
Fecha de Revisión:	29/06/2022
Versión	4.0
Clasificación	Público
Cambios desde la última versión Se actualiza (DTI) Dirección de Tecnologías de la Información a (DIT) Dirección de Infraestructura Tecnológica. Se actualizo el punto 1.1 Objetivos, 1.2 Alcance, 2.2.1 Generales, referente a contenido. Se modifica la tabla de control de versiones.	

TABLA DE CONTENIDOS

SECCIÓN I 4
ASPECTOS GENERALES 4
1.1 Objetivos 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 Instalación de software y prevención contra el software malicioso 5
2.2.1 Generales 5
2.3 Documentos relacionados 6

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

SECCIÓN I
ASPECTOS GENERALES

1.1 Objetivos

Asegurar que el usuario conozca las recomendaciones y las implicaciones sobre el uso de software en cumplimiento a las normas aplicables, con el fin de preservar la integridad, confidencialidad y disponibilidad de los sistemas de información y los equipos de cómputo de usuario final.

1.2 Alcance

Aplicable a todos los usuarios que utilizan y se conectan a la red de TI de la Universidad con equipo propio o de la ejecutora a la cual están adscritos, así como invitados o personal externo contratado para servicios tercerizados que hagan uso de la infraestructura, plataformas tecnológicas y los sistemas de información de la Universidad.

1.3 Definiciones, siglas y acrónimos

- **Antispam**: sistema para prevenir y/o restringir la entrega correo no deseado.
- **Código Malicioso**: es un tipo de código informático o script web dañino diseñado para explotar vulnerabilidades en los sistemas de información o aplicativos 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 (Kaspesrky.com, 2022).
- **ERISI**: Equipo de Respuesta a Incidentes de Seguridad de la Información.
- **Malware**: tipo de software malicioso que infecta a los dispositivos de cómputo o móviles con finalidades diferentes, como extraer información, robo, etc. sin conocimiento del usuario.
- **Rollback**: proceso de regresar un sistema a algún estado previo.
- **SGSI:** Sistema de Gestión de la Seguridad de la Información.
- **Software:** programa o sistema informático que se instalan en computadoras para realizar tareas específicas.
- **TI:** Tecnologías de la Información.
- **Tipo de software:**
    - **Licencia Perpetua.** Se refiere al software que se adquiere hasta la última versión y es propiedad de la Universidad/Ejecutora que compra la licencia de uso, de una versión particular de software, pagando en una sola exhibición el valor completo de dicha licencia. En la mayoría de los casos es necesario adquirir un contrato de soporte para tener acceso a actualizaciones o parches para resolver problemas técnicos o solucionar vulnerabilidades de seguridad, ya que usualmente el periodo de garantía es corto, generalmente 90 días. En

teoría, este tipo de licencias se pueden usar indefinidamente por no tener una vigencia, pero en la práctica la vida útil de una licencia de este tipo es corta y puede variar desde dos hasta cinco años, al final de la cual tenemos que adquirir una nueva licencia de uso para la última versión del software.

- **Suscripción.** Derecho de uso de software donde la Universidad/Ejecutora paga de manera recurrente -generalmente anual, aunque puede ser mensual por la licencia de uso del software. El pago de la suscripción le permite tener acceso a la última versión de este incluyendo correcciones a problemas o vulnerabilidades de seguridad (parches) que se realicen durante la vigencia del contrato y generalmente incluye en el costo de la suscripción el acceso a soporte técnico sin tener que contratar un algún elemento adicional.

- **Universidad:** Universidad Autónoma de Tamaulipas.

SECCIÓN II
POLÍTICA

2.1 Cumplimiento

- NMX-I-27001-NYCE-2015 / Apéndice A / A.12.2 Protección contra el software malicioso (malware).
- NMX-I-27001-NYCE-2015 / Apéndice A / A.12.5 Control de software operacional
- NMX-I-27001-NYCE-2015 / Apéndice A / A.12.6.2 Restricciones en la instalación de software
- NMX-I-27001-NYCE-2015 / Apéndice A / A.18.1.2 Derechos de propiedad intelectual

2.2 Política de Instalación de software y prevención contra el software malicioso

2.2.1 Generales

- Las Facultades, Escuelas, Unidades Académicas, Secretarías, Direcciones, Coordinaciones, Institutos, Departamentos y Divisiones, deberán considerar en su planeación la adquisición para el derecho de uso del software ya sea en licenciamiento anualizado, licencias perpetuas, suscripciones, etc.) relacionadas a sus áreas de pertinencia. Cada una de estas ejecutoras será responsable de:

  1. Realizar de forma periódica la revisión de los aplicativos instalados en los dispositivos de cómputo usados en sus instalaciones y que accedan a la red universitaria, en términos de legalidad y actualizaciones, con el fin de estar en cumplimiento y prevenir incidentes de seguridad de la información.
  2. Elaborar un inventario de los programas de cómputo; con el fin de conocer lo instalado en cada uno de los equipos de cómputo mismo que deberá ser informado a la Dirección de Infraestructura Tecnológica de la Secretaría de Administración cada año.

3. Todo software instalado deberá ser comprobable la vigencia de los derechos de uso.
4. Desinstalar y en su caso borrar software no genuino que no cuenten con un sustento de uso legal.

Lo anterior, a efecto de que el software utilizado en la universidad cumpla con la protección, derechos patrimoniales y uso legítimo establecido en la normatividad aplicable.

- El uso de software no genuinos o sin derechos de uso, vulnera la seguridad de la información al permitir el uso ilegítimo y la posible infiltración de código malicioso, malware, troyanos, virus, software espías, etc., lo que además traerá como consecuencia la transgresión a lo establecido por los artículos 13 fracción XI, 101 al 114, 213 y 231 de la Ley Federal del Derecho de Autor, incurriendo en conductas tipificadas como delitos por los artículos del 424 al 429 del Código Penal Federal. Asimismo, el Órgano Interno de Control podrá implementar las sanciones correspondientes.

- Se recomienda establecer programas de concientización y medidas preventivas del usuario para evitar la descarga de adjuntos o hipervínculos maliciosos en el correo institucional. Así como, evitar navegación de sitios no recomendados y descargas de archivos no seguros.
- Se recomienda la capacitación constante en materia de procedimientos y responsabilidades relacionadas a la protección contra el malware, así como la recuperación de estos ataques.
- Se recomienda la agregación de las computadoras al dominio uat.edu.mx para la actualización constante de parches del sistema operativo y antivirus Microsoft.
- Se recomienda la instalación y actualización periódica de soluciones de antivirus institucionales y en caso externo contar con uno vigente.
- El software que es administrado por la Dirección de Infraestructura Tecnológica deberá ser solicitado a través de la Mesa de Servicios extensión telefónica 2880.
- En caso de incidencia de algún tipo de malware o programa malicioso, deberá reportarse a través de la mesa de servicios para activar el procedimiento a cargo del Equipo de Respuestas a Incidentes de Seguridad de la Información (ERISI). Para los efectos conducentes se da parte a la autoridad/especialista listado en el documento de contactos con autoridades y grupos de especial interés para la seguridad de la información.

2.3 Documentos relacionados

- Reglamento de Seguridad de la Información.
- Acuerdo rectoral por el que se constituye el Comité de Tecnologías de la Información de la Universidad Autónoma de Tamaulipas de fecha 17 de agosto de 2015, publicado en la Gaceta Universitaria N°8 Segunda Etapa del mismo mes y año.

- Artículos 13 fracción XI, 101 al 114, 213 y 231 de la Ley Federal del Derecho de Autor, conductas tipificadas como delitos por los artículos del 424 al 429 del Código Penal Federal.