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 CONTROL ACCESO A LAS REDES Y LOS SERVICIOS DE LA RED

Última Fecha de Actualización: diciembre 07, 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	07/12/2022
Fecha de Revisión:	07/12/2022
Versión	5
Clasificación	Pública
Cambios desde la última versión 2.3 Documentos relacionados: Se agrega la Política de Uso y Responsabilidad de la Cuenta Institucional y cuentas de Gestión y Acceso a Servicios Tecnológicos. Se modifica la tabla de control de versiones.	

TABLA DE CONTENIDOS

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 Objetivo general

Limitar el acceso a usuarios finales y permitir únicamente a usuarios que previamente fueron autorizados para hacer uso de los servicios de red críticos.

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, plataformas tecnológicas y los sistemas de información 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).
- **Lugar de trabajo:** Es cualquier lugar físico donde uno o más usuarios desarrollan sus tareas.
- **Medios de almacenamiento:** Son elementos técnicos destinados a proveer de espacio físico para albergar archivos.
- **SGSI:** Sistema de Gestión de la Seguridad de la Información.
- **Universidad:** Universidad Autónoma de Tamaulipas.
- **CIT:** Coordinación de Informática y Telecomunicaciones.
- **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.
- **HTTPS:** El Protocolo seguro de transferencia de hipertexto.
- **SSH:** Secure Shell, es un protocolo de administración remota.
- **RDP:** Protocolo de Escritorio Remoto.
- **DMZ:** Demilitarized Zone o red perimetral

- SECCIÓN II

POLÍTICA

2.1 Cumplimiento

- NMX-I-27001-NYCE-2015 / Apéndice A / A.9.1.2 Acceso a las redes y los servicios de red.

2.2 Política de Acceso a la red y los servicios de la red

2.2.1 Generales

- Todo acceso deberá estar restringido a menos que este expresamente permitido a los usuarios que administran los activos, servicios de red, sistemas operativos o aplicaciones.

- Deberá estar documentado los servicios y aplicativos que accederán para los permisos correspondientes, el proceso de autorización y roles de los usuarios internos o proveedores a la Universidad con sus responsabilidades.

- El proceso de autorización y roles de los usuarios internos o proveedores a la Universidad, deberá generarse mediante una petición de correo electrónico, al titular del área o coordinador responsable para su previa autorización, enviando la solicitud a la mesa de servicios para su registro y asignación del ticket.

- Para la gestión en la protección de los accesos a las conexiones de red y servicios de red deberán:

    a) Restringir los privilegios de administración a usuarios finales.

    b) Restringir el uso de usuarios genéricos para el acceso con roles y privilegios de administrador.

    c) Asegurar el uso de procedimiento de inicio seguro de sesión.

    d) La autentificación por medio de llaves cifradas utilizando el protocolo de SSH, RDP y HTTPS.

    e) Proteger los servicios por políticas de firewall o zonas DMZs, en su defecto con listas de acceso cuando no este de por medio un Firewall.

    f) Limitar el número de intentos fallidos.

    g) Utilizar mecanismos seguros para la creación de contraseñas.

h) Forzar el cambio periódico de contraseñas al menos cada 6 meses.

- Los usuarios previamente autorizados pueden acceder a los servicios por medio de la infraestructura de la Universidad, los cuales son por servicios cableados o redes inalámbricas que tienen comunicación con los activos, cuando el usuario se encuentra dentro de la red de la Universidad, los medios utilizados para el acceso a los servicios:

    a) El usuario y dispositivo utilizado para acceder a los servicios de red deberá formar parte del dominio y Directorio Activo, para los permisos y roles autorizados

    b) Los dispositivos deberán contar con el antivirus recomendado por la CIT, mantenerlo actualizado, dichas actualizaciones deberán ser descargadas en un sitio de confianza

    c) La conexión en redes cableadas deberá estar dentro de la red de la Universidad y registrada su dirección IP para el control y permisos a los servicios.

    d) Para redes inalámbricas deberá acceder por medio de el usuario de directorio activo para los permisos necesarios. En caso contrario deberá gestionar el permiso de autorización con CIT para solicitar el usuario. Deberá seguir el procedimiento y políticas de redes móviles para acceder a la red.

    e) Los proveedores previamente autorizados pueden acceder por medio del servicio de VPN con el que cuenta la Universidad para acceso externos.

- Los Requerimientos de Autenticación de los usuarios con permisos previamente autorizados deberán utilizar:

    a) Cuenta de Directorio Activo

    b) Autentificación por medio de Radius, Tacacs o Local

    c) Certificado SSL

- Los accesos a los servicios de red deberán ser monitoreados y registrados por el responsable de su servicio o aplicación y registrar los logs de acceso.

2.3 Documentos relacionados

- Reglamento de Seguridad de la Información.
- Política de seguridad para personal visitante o externo.
- Política de Uso y Responsabilidad de la Cuenta Institucional y cuentas de Gestión y Acceso a Servicios Tecnológicos.

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