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 USO Y RESPONSABILIDAD DE LA CUENTA INSTITUCIONAL Y CUENTAS DE GESTIÓN Y ACCESO A SERVICIOS TECNOLÓGICOS.

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/Diciembre/2022
Fecha de Revisión	07/Diciembre/2022
Versión	6.0
Clasificación	Público

Cambios desde la última versión

Se realizan los siguientes cambios:

Se renombra la política, agregando cuentas de gestión y acceso a servicios tecnológicos.

Se modifica el alcance y cumplimiento.

Se incluye el punto 2.3 correspondiente a generales, especificaciones y responsabilidad de la cuenta de gestión y acceso a servicios tecnológicos.

TABLA DE CONTENIDOS

SECCIÓN I

ASPECTOS GENERALES

1.1 Objetivos

Garantizar que los usuarios conozcan el uso y responsabilidad de la cuenta institucional que le permite el acceso autorizado a la red de Tecnologías de la Información Institucional.

1.2 Alcance

Esta política aplica a todo el personal universitario que hace uso de la cuenta institucional, acceden a la infraestructura, plataformas tecnológicas y los sistemas de información de la Universidad y para el personal externo de servicios tercerizados.

1.3 Definiciones, siglas y acrónimos

- **Dominio UAT.EDU.MX**: Nombre único de identificación en Internet de la Universidad Autónoma de Tamaulipas.
- **DIT.** Dirección de Infraestructura Tecnológica.
- **SGSI:** Sistema de Gestión de la Seguridad de la Información.
- **Software:** Programa o sistema informático que se instalan en computadoras para realizar tareas específicas.
- **Universidad:** Universidad Autónoma de Tamaulipas.

SECCIÓN II

POLÍTICA

2.1 Cumplimiento

- NMX-I-27001-NYCE-2015 / Apéndice A / A 9.1.2 Accesos a las redes y a los servicios de la red
- NMX-I-27001-NYCE-2015 / Apéndice A / A.9.2 Gestión del acceso del usuario
- NMX-I-27001-NYCE-2015 / Apéndice A / A 9.3. Responsabilidades del usuario.
- NMX-I-27001-NYCE-2015 / Apéndice A / A 9.4.3 Sistema de administración de contraseñas.
- NMX-I-27001-NYCE-2015 / Apéndice A / A 13 Seguridad en las comunicaciones.

2.2 Uso y responsabilidad de la cuenta institucional.

2.2.1 Generales

- Los tipos de cuentas institucionales se describen en los lineamientos de la gestión de la cuenta institucional universitaria: Cuentas de Personal Activo, Cuentas de Personal Jubilado, Cuentas de Colaboradores Externos y Cuentas de Servicios.
- La autorización para la creación/revocación de cuentas institucionales y privilegios que proporcionarán el acceso a los servicios de tecnología institucionales será de acuerdo con lo establecido en los lineamientos de la gestión de la cuenta institucional universitaria.
- Todos los usuarios mencionados en los lineamientos de la gestión de la cuenta institucional universitaria, debe contar con una cuenta institucional que le otorgue el acceso a los servicios tecnológicos a los que sean autorizados.
- La solicitud de cuentas de colaboradores externos y de servicios con previa autorización del titular del área, se realiza por medio de la Mesa de Servicios de la DIT, quienes registran y asignan un ticket.
- Será causa de suspensión o eliminación de la cuenta institucional conforme lo establecido en los lineamientos de la gestión de la cuenta institucional universitaria.
- Para la depuración de cuentas y privilegios se establecerá un periodo de revisión anual conforme lo establecido en los lineamientos de la gestión de la cuenta institucional universitaria.
- La cuenta de usuario del dominio UAT.EDU.MX es el medio de acceso a los servicios tecnológicos que ofrece la Universidad Autónoma de Tamaulipas, como redes inalámbricas, recursos compartidos o sistemas, esto una vez que son asignados los

privilegios correspondientes por parte de los responsables de dichos servicios o sistemas.

2.2.2 Especificaciones técnicas de la cuenta institucional

La cuenta institucional se compone de: Nombre de usuario (Alias), descripción del nombre y contraseña segura. Esta cuenta se asocia con el correo electrónico con el mismo alias y el dominio (@uat.edu.mx).

- La DIT realiza el proceso de alta de las cuentas de usuario en el dominio UAT.EDU.MX.
- Las cuentas de usuario se protegen con una contraseña y los requisitos que debe cumplir el usuario son los siguientes:
    - No debe contener nombre de usuario (alias) o parte de este.
    - No debe contener nombre o apellidos del usuario, o parte de ellos.
    - Estar formada por 8 caracteres o más, de los cuales:
        - Al menos un carácter en mayúscula de la A a la Z.
        - Al menos un carácter en minúscula de la A a la Z.
        - Al menos un número del 0 al 9.
    - El reinicio de la contraseña se deberá realizar cuando ocurra cualquiera de las siguientes situaciones:
        - El usuario ha extraviado la contraseña y no la recuerda.
        - El usuario utiliza por primera vez su cuenta de usuario del dominio UAT.

    - El reinicio de contraseña lo deberá solicitar por medio de la Mesa de Servicios de la DIT, quienes registran y asignan un ticket, para que se lleve a cabo por parte de Personal Nivel 1, en el módulo del sistema de Mesa de Servicios.

- Se recomienda ampliamente:
    - No reutilizar las ultimas 3 contraseñas utilizadas anteriormente.
    - Cambiar inmediatamente cuando se ha detectado que alguien ha logrado capturar la contraseña.
    - No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos.
    - No escribir las contraseñas en equipos de los que se desconozca su nivel de seguridad.
    - Evitar anotar o guardar la contraseña en lugares de fácil acceso para otras personas.
    - Evitar activar o hacer uso de la utilidad "Recordar contraseña" que ofrecen las aplicaciones.

2.2.3 Responsabilidad del uso de la cuenta institucional

- La cuenta de usuario proporcionada por la DIT es para uso personal e intransferible.
- El buen uso de la cuenta de usuario es responsabilidad de la persona a la que está asignada.
- Una vez entregadas las credenciales de su cuenta institucional, el usuario es el único responsable de todas las operaciones que se realicen con ésta.
- Se recomienda que toda computadora sea agregada al dominio UAT.EDU.MX, a través del personal autorizado por la DIT. A través de este servicio, las computadoras reciben de forma automática las actualizaciones de antivirus, sistema operativo y parches de seguridad.
- Se recomienda ampliamente evitar el uso de programas de cómputo (software) no genuinos o sin derechos de uso, ya que vulnera la seguridad de la información al permitir el uso ilegitimo y la posible infiltración de malware, troyanos, virus, software espías, etc., lo que traería como consecuencia la transgresión a lo establecido en los capítulos I "Reglas generales" y V " De los programas de computación y las bases de datos" de la Ley Federal del Derecho de Autor, incurriendo en conductas tipificadas como delitos mencionados en el Título Vigésimo Sexto "De los delitos en materias de derechos de autor" del Código Penal Federal.

2.3 Cuentas de gestión y acceso a servicios tecnológicos.

2.3.1 Generales

- Los tipos de cuentas de gestión se refieren a cuentas de servicios o cuentas locales que funcionan para la administración de plataformas o aplicativos; y las cuentas de acceso a servicios tecnológicos se refieren a las cuentas de uso de dichas plataformas y aplicativos.
- Los usuarios que gestionan (administración e interacción con el usuario que usa la plataforma o aplicativo) e implementen (despliegue y mantenimiento) las plataformas tecnológicas o aplicativos de cobertura institucional, serán responsables de mantener la seguridad y el control de las cuentas de acceso.
- Los usuarios que gestionan aplicativos o plataformas tecnológicas que no son institucionales, serán responsables de mantener la seguridad y control de las cuentas de administración y acceso de usuarios; se recomienda realizar depuración de cuentas y privilegios de forma anual.
- Para la creación/revocación de cuentas y privilegios que proporcionarán el acceso a los servicios de tecnología será autorizado por el director o titular del área.

- La solicitud de cuentas de colaboradores externos y de servicios para acceso las plataformas tecnológicas o aplicativos de cobertura institucional se realiza por medio de la Mesa de Servicios que aplique, quienes registran y asignan un ticket.

2.3.2 Especificaciones de las cuentas de gestión y acceso a servicios tecnológicos.

- Se recomienda tener un nombre de usuario no asociado con la tecnología.
- Se recomienda que los administradores de los servicios tecnológicos consideren lo siguiente:
- Mantener un control de cuentas de usuarios individuales para mantener la rendición de cuentas.
- Para los aplicativos que tengan la posibilidad de permitir a los usuarios seleccionar y cambiar sus propias contraseñas se recomienda incluir un procedimiento de confirmación que reconozca errores de entrada.
- Las cuentas se protegen con una contraseña y los requisitos que se recomienda ampliamente cumplir son los siguientes:
  - No debe contener nombre de usuario (alias) o parte de este.
  - No debe contener nombre o apellidos del usuario, o parte de ellos.
  - Estar formada por 8 caracteres o más, de los cuales:
    - Al menos un carácter en mayúscula de la A a la Z.
    - Al menos un carácter en minúscula de la A a la Z.
    - Al menos un número del 0 al 9.
  - El reinicio de contraseña lo deberá solicitar al administrador de la plataforma tecnológica o aplicativo.
    - El reinicio de la contraseña se deberá realizar cuando el usuario ha extraviado la contraseña y no la recuerda.
- Se recomienda programar y ejecutar cambios regulares de contraseñas.
- Se recomienda mantener un registro de las contraseñas anteriores y evitar su reutilización.
- Se recomienda que los aplicativos no muestren las contraseñas en la pantalla cuando se estén introduciendo.
- Se recomienda almacenar y transmitir las contraseñas de forma protegida.

2.3.3 Responsabilidad del uso de la cuenta de gestión y acceso a servicios tecnológicos

- La cuenta de usuario proporcionada es para uso personal e intransferible.
- El buen uso de la cuenta de gestión o de acceso a las plataformas o aplicativos de los servicios tecnológicos es responsabilidad de la persona a la que está asignada.

- Una vez entregadas las credenciales de su cuenta, el usuario es el único responsable de todas las operaciones que se realicen con ésta.
- Se recomienda que toda computadora sea agregada al dominio UAT.EDU.MX, a través del personal autorizado por la DIT. A través de este servicio, las computadoras reciben de forma automática las actualizaciones de antivirus, sistema operativo y parches de seguridad.
- Se recomienda ampliamente evitar el uso de programas de cómputo (software) no genuinos o sin derechos de uso, ya que vulnera la seguridad de la información al permitir el uso ilegitimo y la posible infiltración de malware, troyanos, virus, software espías, etc., lo que traería como consecuencia la transgresión a lo establecido en los capítulos I "Reglas generales" y V " De los programas de computación y las bases de datos" de la Ley Federal del Derecho de Autor, incurriendo en conductas tipificadas como delitos mencionados en el Título Vigésimo Sexto "De los delitos en materias de derechos de autor" del Código Penal Federal.

2.4 Documentos relacionados

- Reglamento de Seguridad de la Información.
- Recomendaciones en el uso de dispositivos móviles.
- Lineamientos de Gestión de la Cuenta Institucional Universitaria para empleados.
- Política de control acceso a las redes y servicios de la red.