Ministerio de
Planificación Estratégica y Modernización

Gobierno de Jujuy
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Políticas de Identificación y Autenticación

04
CAPÍTULO

Políticas de Identificación y Autenticación

1.0 OBJETIVO

Garantizar que solo los usuarios y dispositivos debidamente identificados y autenticados tengan acceso a los recursos de tecnología de la información (TI) de conformidad con las políticas, estándares y procedimientos de seguridad de TI.

2.0 POLÍTICA

Esta política es aplicable a todos los departamentos y usuarios de recursos y activos de TI.

2.1 IDENTIFICACIÓN Y AUTENTICACIÓN

El Departamento de TI deberá:

a. Garantizar que los sistemas de información identifiquen y autentiquen de forma única a los usuarios o procesos que actúan en nombre de los usuarios del Gobierno de Jujuy.
b. Asegurarse de que los sistemas de información implementen autenticación multifactor para el acceso a la red de cuentas privilegiadas.
c. Asegurarse de que los sistemas de información implementen autenticación multifactor para el acceso a la red de cuentas sin privilegios.
d. Garantizar que los sistemas de información implementen autenticación multifactor para el acceso local de cuentas privilegiadas.
e. Asegurarse de que los sistemas de información implementen mecanismos de autenticación resistentes a la repetición para el acceso a la red de cuentas privilegiadas.
f. Asegurarse de que los sistemas de información implementen autenticación multifactor para el acceso remoto a cuentas privilegiadas y no privilegiadas, de modo que uno de los factores sea proporcionado por un dispositivo separado del sistema que obtiene acceso y el dispositivo utilice mecanismos criptográficos de seguridad que protejan el token de autenticación principal (clave secreta, clave privada o contraseña de un solo uso) contra el compromiso por amenazas de protocolo que incluyen: escuchas ilegales, repetición, adivinanzas en línea, suplantación de verificador y ataques de man-in-the-middle.
g. Asegúrese de que los sistemas de información acepten y verifiquen electrónicamente las credenciales de Verificación de Identidad Personal (PIV).

2.2 IDENTIFICACIÓN Y AUTENTICACIÓN DEL DISPOSITIVO

El Departamento de TI deberá:

a. Asegurarse de que los sistemas de información identifiquen y autentiquen de forma única todos los dispositivos antes de establecer una conexión de red.

2.3 GESTIÓN DE IDENTIFICADORES

El Departamento de TI, a través de los administradores o encargados de los sistemas de información del departamento, deberá:

a. Asegurarse de que el Gobierno de Jujuy administre los identificadores del sistema de información recibiendo autorización del CISO o encargado de Seguridad Informática para asignar un identificador de individuo, grupo, rol o dispositivo.
b. Seleccionar un identificador único que identifique a un individuo, grupo, función o dispositivo.
c. Asignar el identificador al individuo, grupo, función o dispositivo previsto.
d. Evitar la reutilización de identificadores durante 90 días, salvo que exista alguna política gubernamental más restrictiva que la mencionada.
e. Desactivar el identificador después de 30 días de inactividad.

2.4 GESTIÓN DE AUTENTICADORES

El Departamento de TI deberá:

a. Administrar los autenticadores del sistema de información verificando, como parte de la distribución inicial del autenticador, la identidad del individuo, grupo, rol o dispositivo que recibe el autenticador.
b. Establecer contenido de autenticador inicial para los autenticadores definidos por la organización.
c. Asegurarse de que los autenticadores tengan un mecanismo suficientemente resistente para el uso previsto.
d. Establecer e implementar procedimientos administrativos para la distribución inicial de autenticadores, para autenticadores perdidos, comprometidos o dañados, y para revocar autenticadores.
e. Cambiar el contenido predeterminado de los autenticadores antes de la instalación del sistema de información.
f. Establecer restricciones de vida mínimas y máximas y condiciones de reutilización para los autenticadores.

g. Implementar mecanismos que permitan cambiar/actualizar los autenticadores cada 90 días.
h. Proteger el contenido del autenticador contra divulgación y modificación no autorizadas.
i. Requerir que las personas y los dispositivos implementen las medidas de seguridad específicas para proteger a los autenticadores.
j. Cambiar los autenticadores para cuentas de grupo/rol cuando cambie la membresía en esas cuentas.
k. Asegurarse de que los sistemas de información, **para la autenticación basada en contraseñas**, apliquen una complejidad mínima de contraseña que no debe contener el valor completo del Nombre de cuenta o el valor completo del Nombre del usuario.
l. Asegúrese de que las contraseñas contengan caracteres de **cuatro** de las siguientes cinco categorías, siendo las primeras 4 obligatorias:

    i. Caracteres en mayúsculas de idiomas español (de la A a la Z)
    ii. Caracteres en minúscula de idiomas español (de la a a la z);
    iii. Base 10 dígitos (0 a 9);
    iv. Caracteres no alfanuméricos ~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/ ; y
    v. Cualquier carácter Unicode que esté categorizado como carácter alfabético, pero que no esté en mayúsculas ni en minúsculas.

m. Requerir que las contraseñas tengan una longitud mínima de 14 caracteres.
n. Aplicar al menos un carácter cambiado cuando se crean nuevas contraseñas.
o. Almacenar y transmitir únicamente contraseñas protegidas criptográficamente.
p. Aplicar restricciones de vida mínima y máxima de contraseña de un día y 120 días respectivamente.
q. Prohibir la reutilización de contraseñas durante 12 (doce) generaciones.
r. Permitir el uso de una contraseña temporal para iniciar sesión en el sistema con un cambio inmediato a una contraseña permanente.
s. Asegúrese de que el sistema de información, **para la autenticación basada en PKI**, valide las certificaciones mediante la construcción y verificación de una ruta de certificación hacia una entidad certificadora de confianza aceptada, incluida la verificación de la información del estado del certificado.
t. Hacer cumplir el acceso autorizado a la clave privada correspondiente.
u. Asignar la identidad autenticada a la cuenta del individuo o grupo.
v. Implementar un caché local de datos de revocación para respaldar el descubrimiento y la validación de rutas en caso de que no se pueda acceder a la información de revocación a través de la red.

w. Requerir que el proceso de registro para recibir los accesos/credenciales específicos se lleve a cabo en persona o por un tercero confiable ante las Autoridades del Departamento de TI con autorización de CISO o Encargado de Seguridad.
x. Garantizar que el sistema de información, para la autenticación basada en tokens de hardware, emplee mecanismos que satisfagan los requisitos de calidad de tokens definidos por el Gobierno de Jujuy.

2.5 COMENTARIOS DEL AUTENTICADOR

El Departamento de TI deberá:

a. Asegurarse de que los sistemas de información oculten la retroalimentación de la información de autenticación durante el proceso de autenticación para proteger la información de una posible explotación/uso por parte de personas no autorizadas.

2.6 AUTENTICACIÓN DEL MÓDULO CRIPTOGRÁFICO

El Departamento de TI deberá:

a. Asegurar que los sistemas de información implementen mecanismos de autenticación a un módulo criptográfico que cumplan con los requisitos de las leyes, directivas, políticas, regulaciones, estándares y guías estatales y federales aplicables para dicha autenticación.

2.7 IDENTIFICACIÓN Y AUTENTICACIÓN

El Departamento de TI deberá:

a. Garantizar que los sistemas de información identifiquen y autentiquen de forma única a usuarios, o procesos que actúen en nombre de usuarios, en ambos casos que no sean entidades.
b. Asegurarse de que los sistemas de información acepten y verifiquen electrónicamente las credenciales de Verificación de Identidad Personal (PIV) de otras agencias gubernamentales.
c. Asegurarse de que los sistemas de información acepten únicamente credenciales de terceros aprobadas por la iniciativa el Gobierno Provincial y Nacional.
d. Asegurarse de que la organización emplee únicamente componentes de sistemas de información aprobados por el Gobierno Provincial y Nacional en sistemas de información definidos por el Gobierno de Jujuy para aceptar credenciales de terceros.

3.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los no empleados, incluidos, entre otros, los contratistas, pueden estar sujetos a la rescisión de acuerdos contractuales, a la denegación de acceso a los recursos de TI y a otras acciones, así como a sanciones tanto civiles como penales.

4.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad (DC) y la Secretaría de Innovación Pública (SIP) y/o Encargado de Seguridad de la Información. Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes al DC/SIP. La solicitud debe indicar específicamente el alcance de la excepción junto con la justificación para otorgar la excepción, el posible impacto o riesgo asociado al otorgar la excepción, las medidas de mitigación de riesgos que debe tomar el Departamento de TI, iniciativas, acciones y un cronograma para lograrlo, el nivel mínimo de cumplimiento de las políticas aquí establecidas. El DC/SIP revisará dichas solicitudes; consultar con el departamento solicitante.

5.0 DEPARTAMENTO RESPONSABLE

Oficina principal de información y propietarios de sistemas de información de la Provincia de Jujuy.

6.0 HISTORIAL DE REVISIONES

Fecha	Descripción de Cambio	Crítico
27-05-2024	Draft final del documento	Alejandro Castro Pablo Zalazar