

PROTOCOLO ■■■
PROVINCIAL DE CIBERSEGURIDAD

**Política de
Control de Acceso**

01
CAPÍTULO



Política de Control de Acceso

1.0 OBJETIVO

Garantizar que los controles de acceso estén implementados y cumplan con las políticas, estándares y procedimientos de seguridad de TI.

2.0 POLÍTICA

1. ADMINISTRACIÓN DE CUENTAS

El Departamento de TI deberá:

- a. Identificar y seleccionar los siguientes tipos de cuentas de los sistemas de información para respaldar los objetivos organizacionales y las funciones operativas: individual, compartida, grupal, de sistema, invitada/anónima, de emergencia, desarrollador/fabricante/proveedor, temporal y de servicio.
- b. Asignar administradores de cuentas para las cuentas de los sistemas de información.
- c. Establecer condiciones para la pertenencia a grupos y roles.
- d. Especificar los usuarios autorizados de los sistemas de información, la pertenencia a grupos y roles, y las autorizaciones de acceso (es decir, privilegios) y otros atributos (según sea necesario) para cada cuenta.
- e. Requerir aprobaciones por parte de los propietarios de los sistemas de información para creación de cuentas en los mismos.
- f. Crear, habilitar, modificar, deshabilitar y eliminar cuentas de los sistemas de información de acuerdo con los procedimientos aprobados.
- g. Monitorear el uso de las cuentas de los sistemas de información.
- h. Notificar a los administradores de cuentas cuando las cuentas ya no sean necesarias, cuando los usuarios sean eliminados o transferidos, y cuando se modifique el uso de los sistemas de información.
- i. Autorizar el acceso a los sistemas de información a través de una autorización de acceso válida o uso previsto para los sistemas.
- j. Revisar las cuentas de los sistemas de información para verificar el cumplimiento de los requisitos de administración de cuentas mensualmente.
- k. Establecer un proceso para volver a emitir credenciales de cuentas compartidas/grupales (si se implementan) cuando se eliminen personas del grupo.

- l. Emplear mecanismos automatizados para apoyar la gestión de cuentas de los sistemas de información.
- m. Asegurar que los sistemas de información desactiven automáticamente las cuentas temporales y de emergencia después de su uso.
- n. Asegurar que los sistemas de información deshabiliten automáticamente las cuentas inactivas después de treinta días.
- o. Asegurar que los sistemas de información auditen automáticamente las acciones de creación, modificación, habilitación, deshabilitación y eliminación de cuentas, y notifique al personal de TI correspondiente.

2. APLICACIÓN DEL ACCESO

El Departamento de TI deberá:

- a. Asegurar que los sistemas de información hagan cumplir las autorizaciones aprobadas para el acceso lógico a la información y los recursos de los sistemas de acuerdo con las políticas de control de acceso aplicables.

3. APLICACIÓN DEL FLUJO DE INFORMACIÓN

El Departamento de TI deberá:

- a. Garantizar que los sistemas de información hagan cumplir las autorizaciones aprobadas para controlar el flujo de información dentro de los sistemas y entre sistemas interconectados según la política aplicable.

4. SEPARACIÓN DE TAREAS

El Departamento de TI deberá:

- a. Separar los deberes de los individuos según sea necesario, para prevenir actividades malévolas sin colusión.
- b. Documentar la separación de deberes de las personas.
- c. Definir autorizaciones de acceso a los sistemas de información para soportar la separación de funciones.

5. PRIVILEGIOS MÍNIMOS

El Departamento de TI deberá:

- a. Emplear el principio de menor privilegio, permitiendo solo accesos autorizados para los usuarios (o procesos que actúan en nombre de los

- usuarios) que sean necesarios para realizar las tareas asignadas de acuerdo con los objetivos organizacionales y las funciones operativas.
- b. Autorizar explícitamente el acceso al hardware y software que controla el acceso a los sistemas y reglas de filtrado de enrutadores/firewalls, sistemas de gestión de claves criptográficas, parámetros de configuración de servicios de seguridad y listas de control de acceso.
 - c. Requerir que los usuarios de cuentas o roles de los sistemas de información con acceso a funciones de seguridad definidas por la Repartición o información relevante para la seguridad utilicen cuentas o roles sin privilegios al acceder a funciones que no son de seguridad.
 - d. Restringir las cuentas privilegiadas en los sistemas de información a personal o roles definidos por la Repartición.
 - e. Asegurar que los sistemas de información auditen la ejecución de funciones privilegiadas.
 - f. Asegurar que los sistemas de información impidan que los usuarios sin privilegios ejecuten funciones privilegiadas que incluyan deshabilitar, eludir o alterar las salvaguardias/contramedidas de seguridad implementadas.

6. INTENTOS DE INICIO DE SESIÓN FALLIDOS

El Departamento de TI deberá garantizar que los sistemas de información:

- a. Apliquen un límite de intentos consecutivos de inicio de sesión no válidos por parte de un usuario durante una frecuencia definida por la entidad.
- b. Bloqueen la cuenta/nodo automáticamente durante 48 horas o hasta que un administrador lo libere cuando se excede el número máximo de intentos fallidos.

7. NOTIFICACIÓN DE USO DE LOS SISTEMAS

El Departamento de TI deberá garantizar que los sistemas de información:

- a. Provean a los usuarios un mensaje aprobado o banner de notificación de uso de los sistemas, antes de otorgarles acceso al sistema, que proporcione avisos de privacidad y seguridad consistentes con las leyes, directivas, políticas, regulaciones, estándares y guías estatales y federales aplicables, informando que:
 - i. Los usuarios están accediendo a un sistema de información de Gobierno de Jujuy.
 - ii. El uso de los sistemas de información puede ser monitoreado, registrado y sujeto a auditoría.
 - iii. El uso no autorizado de los sistemas de información está prohibido y sujeto a sanciones penales y civiles.

- iv. El uso de los sistemas de información indica consentimiento al seguimiento y registro.
 - v. No hay derechos a la privacidad.
- b. Mantengan el mensaje de notificación o banner en la pantalla hasta que los usuarios acepten las condiciones de uso y tomen acciones explícitas para iniciar sesión o acceder a los sistemas de información.
- c. Para sistemas de acceso público, el Departamento de TI deberá garantizar que los sistemas de información:
 - i. Provean información de uso, antes de otorgar acceso adicional.
 - ii. Provean referencias, si las hay, a monitoreo, registro o auditoría que sean consistentes con las adaptaciones de privacidad para dichos sistemas que generalmente prohíben esas actividades.
 - iii. Incluyan una descripción de los usos autorizados de los sistemas.

8. BLOQUEO DE SESIÓN

El Departamento de TI deberá garantizar que los sistemas de información:

- a. Eviten un mayor acceso al sistema, iniciando un bloqueo de sesión después de 30 días de inactividad o al recibir una solicitud de un usuario.
- b. Conserven el bloqueo de la sesión hasta que el usuario restablezca el acceso, utilizando los procedimientos de identificación y autenticación establecidos.
- c. Oculten, mediante el bloqueo de sesión, información previamente visible en la pantalla, con una imagen visible públicamente.

9. TERMINACIÓN DE LA SESIÓN

El Departamento de TI deberá:

- a. Asegurar que los sistemas de información finalicen automáticamente la sesión de un usuario después de frecuencia definida por la entidad.

10. ACCIONES PERMITIDAS SIN IDENTIFICACIÓN NI AUTENTICACIÓN

El Departamento de TI deberá:

- a. Identificar las acciones de usuario que se puedan realizar en los sistemas de información sin identificación o autenticación, que sean consistentes con los objetivos organizacionales y funciones operativas.
- b. Documentar y proporcionar fundamentos de respaldo en el plan de seguridad de los sistemas de información, las acciones de usuario que no requieran identificación o autenticación.

11. ACCESO REMOTO

El Departamento de TI deberá:

- a. Establecer y documentar restricciones de uso, requisitos de configuración/conexión y lineamientos de implementación para cada tipo de acceso remoto permitido.
- b. Autorizar el acceso remoto a los sistemas de información, previamente a permitir dichas conexiones.
- c. Asegurar que los sistemas de información monitoreen y controlen los métodos de acceso remoto.
- d. Asegurar que los sistemas de información implementen mecanismos criptográficos para proteger la confidencialidad e integridad de las sesiones de acceso remoto.
- e. Asegurar que los sistemas de información canalicen todos los accesos remotos a través de número definido por la entidad puntos de control administrados de acceso a la red, para reducir el riesgo de ataques externos.
- f. Autorizar la ejecución de comandos privilegiados y el acceso a información relevante para la seguridad, mediante acceso remoto, únicamente para necesidades definidas por la Repartición.
- g. Documentar la justificación de dicho acceso en el plan de seguridad de los sistemas de información.

12. ACCESO INALÁMBRICO

El Departamento de TI deberá:

- a. Establecer restricciones de uso, requisitos de configuración/conexión y guías de implementación para el acceso inalámbrico.
- b. Autorizar el acceso inalámbrico a los sistemas de información, previamente a permitir dichas conexiones.
- c. Asegurar que los sistemas de información protejan el acceso inalámbrico al sistema mediante la autenticación de usuarios y dispositivos y cifrado.

13. CONTROL DE ACCESO PARA DISPOSITIVOS MÓVILES

El Departamento de TI deberá:

- a. Establecer restricciones de uso, requisitos de configuración, requisitos de conexión y guías de implementación para dispositivos móviles controlados por la organización.

- b. Autorizar la conexión de dispositivos móviles a los sistemas de información organizacionales.
- c. Emplear cifrado de dispositivo completo o cifrado de contenedores para proteger la confidencialidad y la integridad de la información en los dispositivos aprobados.

14. USO DE SISTEMAS DE INFORMACIÓN EXTERNOS

El Departamento de TI deberá:

- a. Establecer términos y condiciones consistentes con cualquier organización con la que exista una relación de confianza establecida, que posean, operen y/o mantengan sistemas de información externos, permitiendo a las personas autorizadas:
 - i. Acceder a los sistemas de información desde sistemas de información externos.
 - ii. Procesar, almacenar o transmitir información controlada por la organización, utilizando sistemas de información externos.
- b. Permitir que las personas autorizadas utilicen un sistema de información externo para acceder a los sistemas de información o para procesar, almacenar o transmitir información controlada por la organización, solo cuando la organización:
 - i. Verifique la implementación de los controles de seguridad requeridos en los sistemas externos, según lo especificado en la política y el plan de seguridad de la información de la organización.
 - ii. Conserve los acuerdos de procesamiento o conexión de los sistemas de información aprobados con la entidad organizacional que aloja los sistemas de información externos.

15. EL INTERCAMBIO DE INFORMACIÓN

El Departamento de TI deberá:

- a. Facilitar el intercambio de información, permitiendo a los usuarios autorizados determinar si las autorizaciones de acceso asignadas al socio compartido, coinciden con las restricciones de acceso a la información para circunstancias de intercambio de información definidas por la Repartición donde se requiere la discreción del usuario.
- b. Emplear mecanismos automatizados o procesos manuales definidos por la Repartición para ayudar a los usuarios a tomar decisiones de colaboración/intercambio de información.

16. CONTENIDO PÚBLICAMENTE ACCESIBLE

El Departamento de TI deberá:

- a. Designar personas autorizadas para publicar información en un sistema de información de acceso público.
- b. Capacitar a las personas autorizadas para garantizar que la información de acceso público no contenga información no pública.
- c. Revisar el contenido propuesto, antes de publicarlo en los sistemas de información de acceso público, para garantizar que no se incluya información no pública.
- d. Revisar el contenido de los sistemas de información de acceso público en busca de información no pública frecuencia definida por la Repartición y eliminar dicha información, si la descubre.

3.0 CUMPLIMIENTO

Los empleados que incumplan esta política pueden estar sujetos a medidas disciplinarias que pueden incluir el sumario, así como sanciones civiles y penales. 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). Los departamentos que soliciten excepciones deberán proporcionar dichas solicitudes a la 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 lograr el nivel mínimo de cumplimiento de las políticas aquí establecidas. La SIP revisará dichas solicitudes y concederá al departamento solicitante.

5.0 DEPARTAMENTO RESPONSABLE

Oficina principal de información y propietarios de sistemas de información.

6.0 HISTORIAL DE REVISIONES

Fecha	Descripción de Cambio	Crítico
12-06-2024	Draft final del documento	Alejandro Castro Pablo Zalazar

REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53a - Control de acceso (AC), NIST SP 800-12, NIST 800-46, NIST SP 800-48, NIST SP 800-77, NIST SP 800-94, NIST SP 800-97, NIST SP 800-100, NIST SP 800-113, NIST SP 800-114, NIST SP 800-121, NIST SP 800-124, NIST SP 800-164;

Estándares federales de procesamiento de información (FIPS) 199 del NIST.