Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Políticas de Seguridad Personal

06
CAPÍTULO

Políticas de Seguridad Personal

1.0 OBJETIVO

Garantizar que las políticas de seguridad del personal sean aplicadas al acceso y uso de los recursos y datos de tecnología de la información.

2.0 REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53a – Seguridad del personal (PS), NIST SP 800-12, NIST SP 800-60, NIST SP 800-73, NIST SP 800-78, NIST SP 800-100; Código Electrónico de Regulaciones Federales (CFR): 5 CFR731.106; Estándares federales de procesamiento de información (FIPS)199 y 201; Directiva de la Comunidad de Inteligencia (ICD)704 Normas de seguridad del personal.

3.0 POLÍTICA

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

1. DESIGNACIÓN DE RIESGO DE CARGOS

La tecnología de la información (TI) deberá:

a. Designación de riesgo a todos los cargos.
b. Establecer criterios de selección para las personas que ocupan esos cargos.
c. Revisar y actualizar las designaciones de riesgo de cargos anualmente.

2. SELECCIÓN DE PERSONAL

Los propietarios de aplicaciones y sistemas de departamentos y TI deberán:

a. Validar la identidad de las personas antes de autorizar el acceso a los sistemas de información.
b. Re-validar identidad de los individuos cada dos años, pudiendo disponerse revalidas extraordinarias en caso necesario

c. Asegúrese de que las actividades de selección y revalidación del personal reflejen las leyes, directivas, regulaciones, políticas, estándares, orientación y criterios específicos estatales y federales aplicables establecidos para las designaciones de riesgo de los puestos asignados.

3. CESE DE FUNCIONES DEL PERSONAL

Los departamentos deberán, al terminar las funciones por cualquier causa jurídica, traslado, jubilación, cese de contrato, cesantía o exoneración:

a. Deshabilitar inmediatamente el acceso al sistema de información.
b. Terminar/revocar cualquier autenticador/credencial asociado con el individuo.
c. Realizar entrevistas de salida que incluyan una conversación sobre temas de seguridad de la información definidos por la repartición.
d. Recuperar toda la propiedad relacionada con el sistema de información relacionada con la seguridad.
e. Conservar el acceso a la información y a los sistemas de información anteriormente controlados por la persona desvinculada, por cuestiones de Auditoria, o demás tareas que se requieran.
f. Notificar a la Unidad de Organización a la que pertenecía la persona desvinculada, la obligación de adoptar las medidas referidas precedentemente.

   La propiedad relacionada con el sistema de información incluye, por ejemplo, tokens de autenticación de hardware, manuales técnicos de administración del sistema, llaves, tarjetas de identificación y pases de construcción. Las entrevistas de salida garantizan que las personas desvinculadas comprendan las limitaciones de seguridad impuestas por ser exempleados y que se logre la responsabilidad adecuada por la propiedad relacionada con el sistema de información. Los temas de seguridad de interés en las entrevistas de salida pueden incluir, por ejemplo, recordar a las personas desvinculadas sobre los acuerdos de confidencialidad y las posibles limitaciones en el empleo futuro. Es posible que algunas personas desvinculadas no puedan realizar entrevistas de salida.

La Repartición deberá:

g. Notificar a las personas desvinculadas sobre los requisitos post-empleo aplicables y legalmente vinculantes para la protección de la información.
h. Exigir que las personas desvinculadas despedidas firmen un reconocimiento de los requisitos posteriores al empleo como parte del pro-

ceso de desvinculación según lo indique el Abogado y Recursos Humanos (RR.HH.).

i. Emplear mecanismos automatizados para notificar el cese de servicios de una persona humana.

4. TRASLADO DEL PERSONAL

Los departamentos deberán:

a) Revisar y confirmar la necesidad operativa continua de autorizaciones de acceso físico y lógico actuales a sistemas/instalaciones de información cuando las personas sean reasignadas o transferidas a otras posiciones.
b) Iniciar inmediatamente después de la transferencia formal, acciones de reasignación definidas por la repartición.
c) Modificar la autorización de acceso según sea necesario para corresponder con cualquier cambio en la necesidad operativa debido a una reasignación o transferencia.
d) Notificar a la Unidad de Organización a la que pertenecía la persona transferida, la obligación de adoptar las medidas referidas precedentemente.

Este control se aplica cuando las reasignaciones o traslados de personas son permanentes o de duración tan prolongada que justifican las acciones.

5. PROCEDIMIENTOS DE ACCESO

Los departamentos deberán:

a. Desarrollar y documentar procedimiento de acceso a sistemas de información.
b. Revisar y actualizar semestralmente los procedimientos de acceso.
c. Garantizar que las personas que requieran acceso a la información y a los sistemas de información:

    i. Firmen los acuerdos de acceso adecuados antes de que se le conceda el acceso.
    ii. Vuelvan a firmar las actas de procedimientos de acceso para mantener el acceso a los sistemas de información cuando los mismos hayan sido actualizados. En el caso de personal contratado debe firmarse anualmente. En caso de personal permanente o funcionarios, cuando se produzca un cambio de funciones.

Las actas acuerdos de acceso incluyen, por ejemplo, acuerdos de confidencialidad, acuerdos de uso aceptable, reglas de conducta y acuerdos de conflicto de intereses.

6. SEGURIDAD DEL PERSONAL DE TERCEROS

El Departamento de TI deberá:

a. Establecer y documentar los requisitos de seguridad del personal, incluidas las funciones y responsabilidades de seguridad de los proveedores/consultores externos.
b. Exigir a los proveedores/consultores el cumplimiento de las políticas y procedimientos de seguridad del personal establecidos por la entidad.
c. Requerir que los proveedores/consultores externos notifiquen a de cualquier transferencia de personal o despidos de personal de terceros que posean credenciales y/o insignias, o que tengan privilegios de sistemas de información dentro de las 24 horas.
d. Supervisar el cumplimiento del proveedor.

Los proveedores externos incluyen, por ejemplo, oficinas de servicios, contratistas y otras organizaciones que brindan desarrollo de sistemas de información, servicios de tecnología de la información, aplicaciones subcontratadas y gestión de redes y seguridad.

7. SANCIONES PERSONALES

TI y RRHH deberán:

a. Emplear un proceso de sanción formal de acuerdo con el Estatuto para el Personal de la Administración Pública de la Provincia de Jujuy, Ley 3161 y sus modificatorias, para las personas que no cumplan con las políticas y procedimientos de seguridad de la información establecidos.
b. Notificar dentro de las 24 horas cuando se inicia un proceso formal de sanciones a los empleados, en los términos actuales del artículo 173 incisos 4° a 8° del Estatuto para el Personal de la Administración Pública de la Provincia de Jujuy, Ley 3161.

4.0 CUMPLIMIENTO

Los empleados que violen esta política pueden estar sujetos a medidas disciplinarias, así como sanciones penales, civiles y/o administrativas si correspondieren. Los terceros/proveedores, incluidos, entre otros, los contratistas, pueden es-

tar 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.

5.0 EXCEPCIONES DE POLÍTICA

Las solicitudes de excepciones a esta política serán revisadas por el Director de Ciberseguridad de la Información (DC), 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.

6.0 HISTORIAL DE REVISIONES

Fecha	Descripción de Cambio	Crítico
25-06-2024	Draft final del documento	Alejandro Castro Pablo Zalazar