Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Política de Protección Física y Ambiental

23
CAPÍTULO

Política de Protección Física y Ambiental

1.0 OBJETIVO

Garantizar que los recursos de Tecnología de la Información (TI) estén protegidos por medidas de seguridad físicas y ambientales que impidan la manipulación física, el daño, el robo o el acceso físico no autorizado.

2.0 POLÍTICA

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

1. AUTORIZACIONES DE ACCESO FÍSICO

El Departamento de TI deberá:

a. Desarrollar, aprobar y mantener una lista de personas con acceso autorizado a las instalaciones donde residen los sistemas de información.
b. Emitir credenciales de autorización para el acceso a las instalaciones.
c. Revisar la lista de acceso que detalla el acceso autorizado a las instalaciones por parte de las personas y elimine a las personas de la lista de acceso a las instalaciones cuando el acceso ya no sea necesario.

2. CONTROL DE ACCESO FÍSICO

El Departamento de TI deberá:

a. Hacer cumplir las autorizaciones de acceso físico verificando las autorizaciones de acceso individuales antes de otorgar acceso a las instalaciones.
b. Controlar el ingreso/salida a la instalación usando sistemas/dispositivos y/o medidas de control de acceso físico definidos por la Repartición.
c. Mantener registros de auditoría de acceso físico para puntos de entrada/salida definidos por la Repartición.
d. Proporcionar métodos de seguridad definidas por la Repartición para controlar el acceso a áreas dentro de la instalación oficialmente designadas como de acceso público.

e. Escoltar a los visitantes y monitorear la actividad de los visitantes en áreas especificadas por la Repartición que considere deban tener esta política.
f. Claves seguras, combinaciones y otros dispositivos de acceso físico.
g. Inventario de dispositivos de acceso físico definidos por la Repartición en una frecuencia definida por la Repartición.
h. Cambiar combinaciones y claves en una frecuencia definida por la Repartición y/o cuando se pierden las claves, las combinaciones se ven comprometidas o las personas son transferidas o desvinculadas.

3. PRUEBAS DE PENETRACIÓN DE INSTALACIONES

El Departamento de TI deberá:

a. Emplear un proceso de prueba de penetración que incluya en una frecuencia definida por la Repartición, intentos no anunciados de eludir los controles de seguridad asociados con los puntos de acceso físico a las instalaciones.

4. CONTROL DE ACCESO AL MEDIO DE TRANSMISIÓN

El Departamento de TI deberá:

a. Controlar el acceso físico a líneas de transmisión y distribución del sistema de información definido por la Repartición dentro de las instalaciones de la entidad utilizando métodos de seguridad definidas por la Repartición.

5. CONTROL DE ACCESO PARA DISPOSITIVOS DE SALIDA

El Departamento de TI deberá:

a. Controlar el acceso físico a los dispositivos de salida del sistema de información para evitar que personas no autorizadas obtengan la salida.

   Controlar el acceso físico a los dispositivos de salida incluye, por ejemplo, colocar los dispositivos de salida en habitaciones cerradas u otras áreas seguras y permitir el acceso únicamente a personas autorizadas, y colocar los dispositivos de salida en ubicaciones que puedan ser monitoreadas por el personal. Monitores, impresoras, fotocopiadoras, escáneres, máquinas de fax y dispositivos de audio son ejemplos de dispositivos de salida de sistemas de información.

6. MONITOREO DEL ACCESO FÍSICO

El Departamento de TI deberá:

a. Monitorear el acceso físico a las instalaciones donde reside el sistema de información para detectar y responder a incidentes de seguridad física.
b. Revisar los registros de acceso físico en una frecuencia definida por la Repartición y al ocurrir eventos definidos por la Repartición o posibles indicaciones de eventos; y coordinar los resultados de las revisiones e investigaciones con la capacidad de respuesta a incidentes del Gobierno de Jujuy.

7. REGISTROS DE ACCESO DE VISITANTES

El Departamento de TI deberá:

a. Mantener registros de acceso de visitantes a las instalaciones donde reside el sistema de información para un período de tiempo definido por la Repartición; y revisa los registros de acceso de los visitantes en una frecuencia definida por la Repartición.

8. EQUIPOS DE ENERGÍA Y CABLEADO

El Departamento de TI deberá:

a. Proteger los equipos eléctricos y el cableado eléctrico del sistema de información contra daños y destrucción.
b. Determinar los tipos de protección necesarios para los equipos de potencia y cableado empleados en diferentes ubicaciones tanto internas como externas a las instalaciones gubernamentales y entornos de operación. Esto incluye, por ejemplo, generadores y cableado de energía fuera de edificios, cableado interno y fuentes de energía ininterrumpida dentro de una oficina o centro de datos, y fuentes de energía para entidades autónomas como vehículos y satélites.

9. APAGADO DE EMERGENCIA

El Departamento de TI deberá:

a. Proporcionar la capacidad de cortar la energía al sistema de información o a los componentes individuales del sistema en situaciones de emergencia.

b. Colocar interruptores o dispositivos de cierre de emergencia para facilitar el acceso fácil y seguridad del personal; y proteger la capacidad de corte de energía de emergencia contra activaciones no autorizadas.

10. ENERGÍA DE EMERGENCIA

El Departamento de TI deberá:

a. Proporcionar un suministro de energía ininterrumpida de corto plazo para facilitar un apagado ordenado del sistema de información; transición del sistema de información a energía alternativa a largo plazo en caso de una pérdida de la fuente de energía primaria.
b. Proporcionar una fuente de alimentación alternativa a largo plazo para el sistema de información que sea capaz de mantener la capacidad operativa mínima requerida en caso de una pérdida prolongada de la fuente de energía primaria.

11. ILUMINACIÓN DE EMERGENCIA

El Departamento de TI deberá:

a. Emplear y mantener iluminación de emergencia automática para el sistema de información que se activa en caso de un corte o interrupción del suministro eléctrico y que cubra las salidas de emergencia y las rutas de evacuación dentro de la instalación.
b. Proporcionar iluminación de emergencia para todas las áreas dentro de las instalaciones que respalden misiones esenciales y funciones gubernamentales.

12. PROTECCIÓN CONTRA INCENDIOS

El Departamento de TI deberá:

a. Emplear y mantener dispositivos/sistemas de detección y extinción de incendios para el sistema de información que estén respaldados por una fuente de energía independiente.

   Esto se aplica principalmente a instalaciones que contienen concentraciones de recursos de sistemas de información, incluidos, por ejemplo, centros de datos, salas de servidores y salas de computadoras centrales. Los dispositivos/sistemas de detección y extinción de incendios incluyen, por ejemplo, sistemas de rociadores, extintores de incendios portátiles, mangueras fijas contra incendios y detectores de humo.

13. CONTROLES DE TEMPERATURA Y HUMEDAD

El Departamento de TI deberá:

a. Mantener los niveles de temperatura y humedad dentro de las instalaciones donde reside el sistema de información en niveles aceptables definidos por la Repartición.
b. Monitorear los niveles de temperatura y humedad en una frecuencia definida por la Repartición incluir alarmas o notificaciones de cambios potencialmente perjudiciales para el personal o el equipo.

14. PROTECCIÓN CONTRA DAÑOS POR AGUA

El Departamento de TI deberá:

a. Proteger el sistema de información de daños resultantes de fugas de agua proporcionando válvulas maestras de cierre o aislamiento que sean accesibles, funcionen correctamente y sean conocidas por el personal clave.
   Esto se aplica principalmente a instalaciones que contienen concentraciones de recursos de sistemas de información, incluidos, por ejemplo, centros de datos, salas de servidores y salas de computadoras centrales. Se pueden emplear válvulas de aislamiento además de, o en lugar de, válvulas de cierre maestras para cerrar el suministro de agua en áreas específicas de preocupación, sin afectar a las reparticiones.

15. ENTREGA Y RETIRO

El Departamento de TI deberá:

a. Autorizar, monitorear y controlar la entrada y salida de las instalaciones y mantener registros de los artículos entregados y retirados de las instalaciones.
   Hacer cumplir eficazmente las autorizaciones de entrada y salida de los componentes del sistema de información puede requerir restringir el acceso a las áreas de entrega y posiblemente aislar las áreas del sistema de información y las bibliotecas multimedia.

16. SITIO DE TRABAJO ALTERNO

El Departamento de TI deberá:

a. Emplear controles de seguridad definidos por la Repartición en sitios de trabajo alternos.

b. Evaluar, en la medida de lo posible, la efectividad de los controles de seguridad en los sitios de trabajo alternos.
c. Proporcionar un medio para que los empleados se comuniquen con el personal de seguridad de la información en caso de incidentes o problemas de seguridad.

Los lugares de trabajo alternativos pueden incluir, por ejemplo, otras instalaciones gubernamentales o residencias privadas de empleados. Si bien comúnmente son distintos de los sitios de procesamiento alternativos, los sitios de trabajo alternativos pueden proporcionar ubicaciones alternativas fácilmente disponibles como parte de las operaciones de contingencia. El personal puede definir diferentes conjuntos de controles de seguridad para sitios de trabajo alternativos específicos o tipos de sitios dependiendo de las actividades relacionadas con el trabajo que se llevan a cabo en esos sitios.

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 HISTORIAL DE REVISIONES

Fecha	Descripción de Cambio	Participantes
07/08/2024	Revisión inicial	Alejandro Castro, Pablo Zalazar
08/08/2024	Visado, y corrección de errores	Alejandro Castro.

6.0 REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST):NIST SP 800-53a – Protección física y ambiental (PE), NIST SP 800-46, NIST SP 800-73, SP NIST 800-76, SP NIST 800-78, SP NIST 800-116;Directiva de la Comunidad de Inteligencia (ICD):704 705; Departamento de Defensa (DoD): Instrucción 5200.39 Protección de información crítica del programa (CPI); Publicación federal de gestión de identidad, credenciales y acceso (FICAM): Verificación de identidad personal (PIV) en el sistema de control de acceso empresarial (E-PACS) (2012)