Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Estándar de IT: Política de Gestión de Configuración

11
CAPÍTULO

Estándar de IT:
Política de Gestión de Configuración

1.0 OBJETIVO

Garantizar que los recursos de tecnología de la información (TI) estén inventariados y configurados 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.

1. CONFIGURACIÓN BASE

El Departamento de TI deberá:

a. Desarrollar, documentar y mantener bajo control de configuración, una línea base de configuraciones de los sistemas de información.
b. Revisar y actualizar la configuración base de los sistemas de información en una frecuencia definida por la Repartición.
c. Revisar y actualizar la configuración base del sistema de información cuando sea necesario como resultado de alguna circunstancia o evento definido por la Repartición y como parte integral de las instalaciones y actualizaciones de los componentes del sistema de información.
d. Conservar una versión anterior de las configuraciones básicas de los sistemas de información para respaldar el rollback.

2. CONTROL DE CAMBIO DE CONFIGURACIÓN

El Departamento de TI deberá:

a. Determinar los tipos de cambios en el sistema de información que están controlados por la configuración.
b. Revisar los cambios propuestos controlados por la configuración del sistema de información y aprobar o desaprobar dichos cambios teniendo en cuenta explícitamente los análisis de impacto en la seguridad.

c. Documentar las decisiones de cambio de configuración asociadas al sistema de información.
d. Implementar cambios aprobados controlados por la configuración en el sistema de información.
e. Conservar registros de cambios controlados por la configuración en el sistema de información en un período de tiempo de cinco (5) años.
f. Auditar y revisar actividades asociadas con cambios controlados por la configuración del sistema de información.
g. Coordinar y supervisar las actividades de control de cambios de configuración a través de un órgano de control de cambios de configuración definido por la Repartición (sea interno o externo que convoca en una frecuencia que resulte adecuada a las necesidades de la Repartición) que convoca en una frecuencia definida por la Repartición, bajo condiciones de cambio de configuración definidas por la Repartición.
h. Probar, validar y documentar los cambios en el sistema de información antes de implementar los cambios en el sistema operativo.

3. ANÁLISIS DE IMPACTO EN LA SEGURIDAD

El Departamento de TI deberá:

a. Analizar los cambios en el sistema de información para determinar los posibles impactos en la seguridad antes de la implementación del cambio.

4. RESTRICCIONES DE ACCESO AL CAMBIO

El Departamento de TI deberá:

a. Definir, documentar, aprobar y hacer cumplir las restricciones de acceso físico y lógico asociadas con cambios en el sistema de información.

5. AJUSTES DE CONFIGURACIÓN

El Departamento de TI deberá:

a. Establecer y documentar los ajustes de configuración para las soluciones tecnológicas de la información empleados dentro del sistema de información utilizando listas de verificación de configuración de seguridad definidas por la Repartición que reflejen el modo más restrictivo compatible con los requisitos operativos.

b. Implementar los ajustes de configuración.
c. Identificar, documentar y aprobar cualquier desviación de los ajustes de configuración establecidos para componentes del sistema de información definidos por la Repartición en requisitos operativos definidos por la misma.
d. Monitorear y controlar los cambios en los ajustes de configuración de acuerdo con las políticas y procedimientos.

6. MÍNIMA FUNCIONALIDAD

El Departamento de TI deberá:

a. Configurar el sistema de información para proporcionar sólo capacidades esenciales.
b. Revisar trimestralmente el sistema de información para identificar funciones, puertos, protocolos y servicios innecesarios y/o no seguros.
c. Deshabilitar funciones, puertos, protocolos y servicios dentro del sistema de información que se consideren innecesarios y/o inseguros.
d. Impedir la ejecución del programa de acuerdo con las políticas relativas al uso del programa de software y las restricciones y reglas que autorizan los términos y condiciones de uso del programa de software.
e. Identificar programas de software no autorizados para ejecutarse en sistemas de información.
f. Emplear una política de denegar todo y permitir por excepción para la ejecución de programas de software autorizados en el sistema de información.
g. Revisar y actualizar la lista de programas de software autorizados anualmente.

7. INVENTARIO DE COMPONENTES DEL SISTEMA DE INFORMACIÓN

El Departamento de TI deberá:

a. Desarrollar y documentar un inventario de los componentes del sistema de información que:

    i. Refleja fielmente el sistema de información actual.
    ii. Incluir todos los componentes dentro del límite de autorización del sistema de información.
    iii. Esté en el nivel de granularidad que se considere necesario para el seguimiento y la presentación de informes.
    iv. Incluir información que se considere necesaria para lograr una rendición de cuentas eficaz de los componentes del sistema de información.

b. Revisar y actualizar el inventario de componentes del sistema de información en una frecuencia definida por la Repartición.
c. Actualizar el inventario de componentes del sistema de información como parte integral de las instalaciones, remociones y actualizaciones del sistema de información.
d. Emplear mecanismos automatizados trimestralmente para detectar la presencia de componentes de hardware, software y firmware no autorizados dentro del sistema de información.
e. Tomar las siguientes acciones cuando se detecten componentes no autorizados:

    i. Deshabilitar el acceso a la red por parte de dichos componentes, o
    ii. Aislar los componentes y notificar al encargado de seguridad información y al propietario del sistema.

f. Verificar que todos los componentes dentro del límite de autorización del sistema de información no estén duplicados en otros inventarios de componentes del sistema de información.

8. PLAN DE GESTIÓN DE LA CONFIGURACIÓN

TI deberá desarrollar, documentar e implementar un plan de gestión de la configuración para el sistema de información que:

a. Aborde roles, responsabilidades, procesos y procedimientos de gestión de configuración.
b. Establece un proceso para identificar elementos de configuración a lo largo del ciclo de vida de desarrollo del sistema y para gestionar la configuración de los elementos de configuración.
c. Define los elementos de configuración para el sistema de información y coloca los elementos de configuración bajo gestión de configuración.
d. Protege el plan de gestión de configuración contra divulgación y modificaciones no autorizadas.

9. RESTRICCIONES DE USO DEL SOFTWARE

El Departamento de TI deberá:

a. Utilizar el software y la documentación asociada de acuerdo con los acuerdos contractuales y las leyes de derechos de autor.
b. Realizar un seguimiento del uso del software y la documentación asociada protegidos por licencias de cantidad para controlar la copia y distribución.

c. Controlar y documentar el uso de la tecnología de intercambio de archivos peer-to-peer (o punto a punto) para garantizar que esta capacidad no se utilice para la distribución, exhibición, ejecución o reproducción no autorizada de trabajos protegidos por derechos de autor.

10. SOFTWARE INSTALADO POR EL USUARIO

El Departamento de TI deberá:

a. Establecer políticas que regulen la instalación de software por parte de los usuarios.
b. Hacer cumplir las políticas de instalación de software controlando el acceso privilegiado y bloqueando la ejecución de archivos mediante la política aplicada por el servicio de directorio y/o la lista blanca de aplicaciones.
c. Supervisar el cumplimiento de las políticas en una frecuencia trimestral.

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 FECHA DE EMISIÓN / FECHA DE REVISIÓN

Fecha	Descripción de Cambio	Crítico
10/07/2024	Draft final del documento	Alejandro Castro Pablo Zalazar
15/07/2024	Revisión, corrección de errores, y agregado de comentarios.	Alejandro Castro

6.0 REFERENCIA

Publicación especial (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53a – Gestión de configuración (CM)