Ministerio de
Planificación Estratégica y Modernización

Gobierno de Jujuy
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Estándar de TI: Estándar Configuración Segura

15
CAPÍTULO

Estándar de TI:
Estándar Configuración Segura

1.0 Propósito y Beneficios

El propósito de esta norma es establecer configuraciones de referencia para los sistemas de información que son propiedad y/u operados por la Repartición. La implementación efectiva de este estándar maximizará la seguridad y minimizará el riesgo potencial de acceso no autorizado a la información y la tecnología.

2.0 Alcance

Esta norma se aplica a todos los sistemas de información que son propiedad de la Repartición y/u operados por ella o en nombre de ella. Los sistemas de laboratorio, como los utilizados para investigación o análisis forense digital, pueden requerir una consideración especial; sin embargo, este estándar debe aplicarse de manera obligatoria, a menos que hacerlo inhiba las funciones principales de estos sistemas o no sea técnicamente factible.

3.0 Declaración de Información

Se deben utilizar perfiles de configuración segura estándar, basados en una o más de las pautas de consenso de la industria que se enumeran a continuación, además de las pautas de seguridad más recientes del proveedor. Las modificaciones al perfil deben basarse en la necesidad gubernamental, la política o el cumplimiento de estándares, desarrollarse en consulta con el Oficial de Seguridad de la Información/Encargado de seguridad designado, documentarse y conservarse para fines de auditoría.

Directrices de consenso de la industria

- Puntos de referencia del Centro de Seguridad de Internet (CIS)
- Programa de lista de verificación nacional del Instituto Nacional de Ciencia y Tecnología (NIST)

La configuración inicial, la instalación del software y la configuración de seguridad de los nuevos sistemas deben realizarse en un entorno seguro aislado de otros sistemas operativos con protocolos de comunicación mínimos habilitados.

Los cambios en las configuraciones se identifican, proponen, revisan, analizan formalmente para determinar el impacto en la seguridad, se prueban y aprueban antes de su implementación de acuerdo con los procedimientos de gestión de cambios. Las personas que realizan análisis de impacto en la seguridad poseen las habilidades y la experiencia técnica necesarias para analizar los cambios en los sistemas de información y las ramificaciones de seguridad asociadas.

Las entidades deben mantener planes de gestión de la configuración que definan procesos y procedimientos detallados sobre cómo se utiliza la gestión de la configuración para respaldar las actividades seguras del ciclo de vida del desarrollo del sistema a nivel del sistema de información. Los planes de gestión de la configuración normalmente se desarrollan durante la fase de desarrollo/adquisición del ciclo de vida de desarrollo del sistema seguro.

Debe existir un proceso de monitoreo de configuración para identificar componentes del sistema no descubiertos o no documentados, configuraciones incorrectas, vulnerabilidades y cambios no autorizados.

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 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.

5.0 Historial de revisiones

Fecha	Descripción de Cambio	Crítico
29/07/2024	Documento inicial, primera revisión	Alejandro Castro, Pablo Zalazar

6.0 Documentos relacionados

Instituto Nacional de Estándares y Tecnología (NIST) 800-128, Guía para la gestión de la configuración de sistemas de información centrada en la seguridad