Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Estándar de IT: Política de Integridad de Sistemas e Información

10
CAPÍTULO

Estándar de IT: Política de Integridad de Sistemas e Información

1.0 OBJETIVO

Garantizar que los recursos y sistemas de información de tecnología de la información (TI) se establezcan con monitoreo de la integridad del sistema para incluir áreas de preocupación como malware, fallas en aplicaciones y códigos fuente, alertas proporcionadas por la industria y solución de problemas de integridad detectados o divulgados.

2.0 POLÍTICA

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

1. SOLUCIÓN DE DEFECTOS

El Departamento de TI deberá:

a. Identificar, reportar y corregir fallas en los sistemas de información.
b. Testear las actualizaciones de software y firmware relacionadas con la corrección de fallas para determinar su efectividad y posibles efectos secundarios antes de la instalación.
c. Instalar actualizaciones de software y firmware relevantes para la seguridad dentro de un tiempo sugerido de 30 días desde el lanzamiento de las actualizaciones.
d. Incorporar la corrección de fallas en el proceso de gestión de la configuración, de acuerdo con la Política de Gestión de Configuraciones.
e. Emplear mecanismos automatizados en una frecuencia definida por la Repartición para determinar el estado de los componentes del sistema de información con respecto a la corrección de fallas.

2. PROTECCIÓN DE CÓDIGO MALICIOSO

El Departamento de TI deberá:

a. Emplear mecanismos de protección de códigos maliciosos en los puntos de entrada y salida del sistema de información para detectar y erradicar códigos maliciosos.

b. Actualizar los mecanismos de protección de códigos maliciosos cada vez que haya nuevas versiones disponibles de acuerdo con la política y los procedimientos de gestión de configuración.
c. Configurar mecanismos de protección de código malicioso para:

    i. Realizar escaneos periódicos del sistema de información en una frecuencia definida por la Repartición y escaneos en tiempo real de archivos de fuentes externas en el punto final; puntos de entrada/salida de la red a medida que los archivos se descargan, abren o ejecutan de acuerdo con la política de seguridad.
    ii. Bloquear código malicioso, poner en cuarentena código malicioso, enviar alerta al encargado u oficial de la Seguridad de la Información, tomando las acciones pertinentes en respuesta a la detección de códigos maliciosos.
    iii. Abordar la recepción de falsos positivos durante la detección y erradicación de códigos maliciosos y el consiguiente impacto potencial en la disponibilidad del sistema de información.

3. MONITOREO DEL SISTEMA DE INFORMACIÓN

El Departamento de TI deberá:

a. Monitorear el sistema de información para detectar:

    i. Ataques e indicadores de posibles ataques.
    ii. Conexiones locales, de red y remotas no autorizadas.

b. Identificar el uso no autorizado del sistema de información mediante técnicas y métodos definidos.
c. Implementar dispositivos de monitoreo ubicaciones estratégicas dentro de la arquitectura de un sistema de información para recolectar información relevante determinada por la Repartición y en ubicaciones ad hoc dentro del sistema para rastrear tipos específicos de transacciones de interés para la Repartición.
d. Proteger la información obtenida de las herramientas de monitoreo de intrusiones contra el acceso, modificación y eliminación no autorizados.
e. Aumentar el nivel de actividad de monitoreo del sistema de información siempre que haya una indicación de un mayor riesgo para las operaciones y los activos, los individuos, otras organizaciones o en base a información de aplicación de la ley, información de inteligencia u otras fuentes creíbles de información.
f. Obtener opinión legal con respecto a las actividades de monitoreo del sistema de información de acuerdo con las leyes, directivas, políticas o regulaciones nacionales y provinciales aplicables.

g. Proporcionar información de monitoreo del sistema de información al personal autorizado o unidades de gubernamentales según sea necesario.

4. ALERTAS GENERADAS POR EL SISTEMA

El Departamento de TI deberá garantizar que:

a. El sistema de información que puede generarse a partir de una variedad de fuentes, incluidos, por ejemplo, registros de auditoría o entradas de mecanismos de protección de códigos maliciosos, mecanismos de detección o prevención de intrusiones o dispositivos de protección de límites como firewalls, puertas de enlace y enrutadores, se difundirá a personal o unidades gubernamentales autorizados que tomarán las medidas adecuadas ante la(s) alerta(s).
b. Las alertas se transmitirán por teléfono, mensajes de correo electrónico o mensajes de texto, según sea necesario. El personal en la lista de notificaciones puede incluir administradores de sistemas, encargados de áreas, propietarios de sistemas o funcionarios de seguridad del sistema de información.

5. ALERTAS, AVISOS Y DIRECTIVAS DE SEGURIDAD

El Departamento de TI deberá:

a. Recibir alertas, avisos y directivas de seguridad del sistema de información de entidades externas definidas por la Repartición y el MPEyM, de forma continua.
b. Generar alertas, avisos y directivas de seguridad interna según se considere necesario.
c. Difundir alertas, avisos y directivas de seguridad para: personal o roles definidos por la Repartición, sobre elementos definidos por la Repartición dentro de la organización, organizaciones externas definidas por la Repartición.
d. Implementar las directivas de seguridad de acuerdo con los plazos establecidos, o notificar al organismo emisor el grado de incumplimiento.

6. INTEGRIDAD DEL SOFTWARE, FIRMWARE E INFORMACIÓN

El Departamento de TI deberá:

a. Emplear herramientas de verificación de integridad para detectar cambios no autorizados en software, firmware e información definidos por la Repartición;

b. Asegurar que el sistema de información realice una verificación de integridad de software, firmware e información definidos por la Repartición al inicio y/o al producirse estados de transición definidos por la Repartición o eventos relevantes para la seguridad, en una frecuencia definida por la Repartición.
c. Incorporar la detección de cambios no autorizados cambios relevantes para la seguridad definidos por la Repartición y el MPEyM en el sistema de información en la capacidad de respuesta a incidentes.

7. PROTECCIÓN CONTRA EL SPAM

El Departamento de TI deberá:

a. Emplear mecanismos de protección contra spam en los puntos de entrada y salida del sistema de información para detectar y tomar medidas ante mensajes no solicitados.
b. Actualizar los mecanismos de protección contra spam cuando haya nuevas versiones disponibles de acuerdo con la política y los procedimientos de gestión de configuración.
c. Gestionar los mecanismos de protección contra spam de forma centralizada.
d. Garantizar que los sistemas de información actualicen automáticamente los mecanismos de protección contra spam.

8. VALIDACIÓN DEL INGRESO DE INFORMACIÓN

El Departamento de TI deberá:

a. Asegurar el sistema de información:
    i. Comprobar la validez de ingresos/entradas de registros de información definidas por la Repartición.
    ii. Proporcionar una capacidad de anulación manual para la validación de ingresos de registros definidos por el MPEyM.
    iii. Restringir el uso de la capacidad de anulación manual a solo personas autorizadas definidas por la Repartición ante el MPEyM.
    iv. Auditar el uso de la capacidad de anulación manual a cargo del MPEyM.
    v. Revisar y resolver errores de validación de ingresos de registros.
    vi. Documentar y seguir los procedimientos correspondientes que reflejen los objetivos del sistema cuando se reciben el ingreso de registros no válidos.

9. MANEJO DE ERRORES

El Departamento de TI deberá:

a. Asegurar el sistema de información:

   i. Generar mensajes de error que brindan información necesaria para acciones correctivas sin revelar información que pueda ser explotada por adversarios.
   ii. Revelar mensajes de error sólo al personal o roles definidos por la Repartición, y las auditorías externas facultadas a tal fin.

10. MANEJO Y RETENCIÓN DE INFORMACIÓN

El Departamento de TI deberá:

a. Manejar y retener información dentro del sistema de información y la información generada por el sistema de acuerdo con las leyes, directivas, políticas, regulaciones, estándares y requisitos operativos nacionales y provinciales aplicables.

11. PROTECCIÓN DE LA MEMORIA

El Departamento de TI deberá:

a. Asegurar que el sistema de información implemente salvaguardias de seguridad definidas por la Repartición para proteger su memoria de la ejecución de código no autorizado.

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). 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
05/07/2024	Draft final del documento	Alejandro Castro Pablo Zalazar
11/07/2024	Agregado de comentarios, corrección de errores.	Alejandro Castro

6.0 REFERENCIA

Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST): NIST SP 800-53a: integridad del sistema y de la información (SI), NIST SP 800-12, NIST SP 800-40, NIST SP 800-45, NIST SP 800-83, NIST SP 800-61, NIST SP800-83, NIST SP 800-92, NIST SP 800-100, NIST SP 800-128, NIST SP 800-137, NIST SP 800-147, NIST SP 800-155