Ministerio de
Planificación Estratégica y Modernización

Gobierno de JUJUY
Cerca de la gente

PROTOCOLO
PROVINCIAL DE CIBERSEGURIDAD

Respuesta a Ciberincidentes

29
CAPÍTULO

Respuesta a Ciberincidentes

1.0 Propósito y Beneficios

Este estándar describe los pasos generales para responder a incidentes de seguridad informática. Además de proporcionar un flujo de proceso estandarizado, (1) identifica las partes interesadas en la **respuesta a incidentes (a partir de aquí en adelante "RI")** y establece sus funciones y responsabilidades; (2) describe las fuentes desencadenantes del incidente, los tipos de incidentes y los niveles de gravedad del incidente; y (3) incluye requisitos para pruebas anuales, actividades de lecciones aprendidas posteriores al incidente y recopilación de métricas de RI para su uso para medir la efectividad de la RI.

Los objetivos de RI, tal como se describen en este estándar, son:

- Confirmar si ocurrió un incidente;
- Proporcionar un proceso de notificación de incidentes definido;
- Promover la acumulación y documentación de información veraz;
- Establecer controles para la recuperación y el manejo adecuado de la evidencia;
- Contener el incidente y detener cualquier actividad no deseada de forma rápida y eficaz;
- Minimizar la interrupción de las operaciones de la red;
- Proporcionar informes precisos y recomendaciones útiles a la dirección; y
- Prevenir y/o mitigar la ocurrencia de futuros incidentes.

2.0 Declaración de información

2.1 FUNCIONES Y RESPONSABILIDADES DE LAS PARTES INTERESADAS EN RI

Para responder eficazmente a un incidente de seguridad informática, es fundamental que todas las partes interesadas de RI comprendan plenamente no sólo sus funciones y responsabilidades en el proceso de RI, sino también las funciones y responsabilidades de cada parte interesada de RI. Esto es necesario para (1) evitar la duplicación de esfuerzos; (2) minimizar las lagunas procesales que puedan ocurrir; y (3) garantizar una respuesta rápida a incidentes de seguridad informática.

Las partes interesadas en RI incluyen:

1. **Responsable de seguridad de la información**: El Director de Ciberseguridad (DC) asumirá la coordinación general de la RI, incluida la escalada de un incidente. El DC lidera los servicios de respuesta a incidentes para la organización.
2. **Liderazgo de la entidad:** Proporciona principalmente supervisión de RI, siendo su Oficial de Seguridad de la Información (ISO) o el encargado el más "práctico" en términos de actividades de gestión de RI.
3. **Centro de operaciones de seguridad:** El Equipo de Operaciones de Seguridad (EOS) sirve como un grupo central para la detección, análisis, seguimiento, respuesta y notificación de amenazas e incidentes cibernéticos. El EOS responde a los incidentes proporcionando RI técnico práctico y recomendará medidas para que el personal remedie y mitigue de manera que reduzca la probabilidad de futuros incidentes.

   Además, el EOS facilita la colaboración y el intercambio de información con otras Reparticiones que puedan estar experimentando incidentes iguales o similares, para ayudar a resolver el problema más rápidamente que si se hiciera por separado. El EOS recopila información sobre los tipos de vulnerabilidades que se están explotando y la frecuencia de los ataques y comparte información preventiva para ayudar a otras reparticiones a protegerse de ataques similares.
4. **Primeros auxilios**: Se recurrirá al personal de TI, como administradores de red, administradores de sistemas y otro personal técnico, según sea necesario, para brindar soporte y respuesta táctica al Equipo de Operaciones de Seguridad. Todo análisis forense digital debe ser realizado por el EOS o bajo su dirección.
5. **Equipos de respuesta a incidentes de la Repartición:** Deben estar listos equipos predefinidos que incluyan, como mínimo, personal de la Dirección o superior Autoridad, del área Legal o Asuntos Jurídicos y Responsable de Comunicaciones o Relaciones Públicas. En algunos casos, pueden verse involucrados Recursos Humanos o Personal.
6. **Entidades Externas**: En consulta con el Equipo de Operaciones de Seguridad, las entidades externas pueden realizar actividades prácticas de RI, como actividades de respuesta de investigación, o pueden proporcionar orientación. Por ejemplo, un proveedor de soluciones de seguridad puede brindar asistencia sobre la configuración de los dispositivos de seguridad. Las entidades externas incluyen vendedores, proveedores de servicios o autoridades encargadas de hacer cumplir la ley, incluidos, entre otros:

   - Ministerio de Seguridad nacional o provincial;
   - Fuerzas de seguridad federales o provinciales (Delitos Informáticos)
   - Proveedores de servicios de Internet

- Proveedores de soluciones de seguridad
- Proveedores titulares de datos

2.2 FLUJO DE RI

Este flujo de proceso de RI cubre cómo responder a situaciones específicas para que las partes interesadas de RI garanticen una respuesta efectiva y eficiente. El enfoque del proceso de RI es erradicar el problema lo más rápido posible, mientras se recopila inteligencia procesable, para restaurar las funciones gubernamentales, mejorar la detección y evitar que vuelva a ocurrir. Una Repartición puede adoptar el flujo de proceso de RI de seis pasos como se muestra a continuación.[1]:

Figura 4.1 – Flujo del proceso de respuesta a incidentes

Paso 1: preparación

La planificación y preparación adecuadas para un incidente antes de que ocurra garantiza un proceso de RI más eficaz y eficiente. Las actividades asociadas con este paso incluyen el establecimiento de equipos de RI; actualizar herramientas, políticas/procedimientos y formularios/listas de verificación de RI; y garantizar que los procedimientos de comunicación de RI y las listas de contactos de las partes interesadas de RI sean precisos y estén actualizados. Una entidad debe tener una Lista de Contactos definida y actualizada y establecer múltiples canales de comunicación con todas las entidades e individuos en la Lista de Contactos de RI.

Una Repartición debe asignar la responsabilidad de un punto de contacto central para coordinar la identificación y la presentación de informes a DC. Normalmente, esto lo realiza el Encargado de seguridad designado de la Repartición. Según la Política de seguridad de la información, todos los empleados deben informar

1 Basado en el manejo de incidentes del Instituto SANS paso a paso

sospechas de incidentes o debilidades de seguridad de la información a la autoridad correspondiente al Encargado de seguridad designado.

El Equipo de Operaciones de Seguridad establecerá Procedimientos Operativos Estándar (SOP) para RI para reflejar los estándares y las mejores prácticas globales. Estos SOP se seguirán durante la respuesta a incidentes. Cualquier excepción debe documentarse. El Equipo de Operaciones de Seguridad debe examinar y validar periódicamente las herramientas y técnicas utilizadas para la RI. Para funcionar de manera eficiente y efectiva, el proceso de RI debe probarse periódicamente. Esto debe ocurrir al menos una vez al año. Estas pruebas se pueden lograr con capacitación sobre incidentes simulados o ejercicios prácticos utilizando escenarios realistas para proporcionar un esquema de alto nivel y un recorrido sistemático del proceso de RI y, en la medida de lo posible, deben incluir a todas las partes interesadas de RI. Estos escenarios de capacitación deben incluir 'puntos de discusión' específicos que representen oportunidades clave de aprendizaje e incorporar lecciones aprendidas, que luego puedan integrarse en el proceso de RI como parte de su revisión.

Paso 2: Identificación

La identificación implica la revisión de anomalías para determinar si ha ocurrido o no un incidente y, si ha ocurrido, determinar la naturaleza del incidente. La identificación comienza con un evento, una anomalía que se ha informado o detectado en un sistema o red. La detección se puede lograr a través de fuentes técnicas (por ejemplo, personal de operaciones, software antivirus), fuentes no técnicas (por ejemplo, informes y concientización sobre la seguridad del usuario) o ambas.

Es importante reconocer que no todos los eventos de la red o del sistema serán un incidente de seguridad. Se debe asignar un responsable para determinar si hay un incidente, clasificarlo y escalarlo según sea necesario. Normalmente, será el representante de seguridad designado por la Unidad de Organización.

Para ser eficaz en RI, los incidentes deben clasificarse y derivarse lo antes posible a las partes interesadas de RI adecuadas para promover la colaboración y el intercambio de información. La clasificación de incidentes requiere el uso de categorías de incidentes establecidas junto con una matriz de gravedad de incidentes como medio para priorizar los incidentes y determinar las actividades de RI apropiadas.

CATEGORÍAS DE INCIDENTES

Es importante categorizar los incidentes comunes experimentados en toda la Repartición. Al hacerlo, las partes interesadas en RI pueden enfocar mejor sus actividades de RI. Cabe señalar que los incidentes pueden tener más de una categoría y la categorización puede cambiar a medida que se desarrolla la investigación. Una entidad puede adoptar los seis (6) US-CERT2categorías de incidentes de la siguiente manera:

Categorías de incidentes		
Categoría	**Nombre**	**Descripción**
0	Ejercicio/Pruebas de defensa de red	Se utiliza durante ejercicios nacionales y provinciales e internacionales y pruebas de actividad aprobadas de defensas o respuestas de redes internas/externas.
1	Acceso no autorizado	Un individuo obtiene acceso lógico o físico sin permiso a una red, sistema, aplicación, datos u otro recurso del gobierno local.
2	Denegación de servicio	Un ataque que impide o perjudica con éxito la funcionalidad normal autorizada de redes, sistemas o aplicaciones al agotar los recursos. Esta actividad incluye ser víctima o participar en la Denegación de Servicio (DoS).
3	Código malicioso	Instalación exitosa de software malicioso (p. ej., virus, gusano, caballo de Troya u otra entidad maliciosa basada en código) que infecta un sistema operativo o una aplicación.
4	Uso inadecuado	Una persona que, a sabiendas o sin saberlo, viola las políticas aceptables de uso de la informática.

2 http://www.us-cert.gov/government-users/reporting-requirements

Categorías de incidentes		
Categoría	**Nombre**	**Descripción**
5	Escaneos / Sondas / Intentos de Acceso	Incluye cualquier actividad que busque acceder o identificar la computadora de una entidad, puertos abiertos, protocolos, servicios o cualquier combinación para su posterior explotación. Esta actividad no resulta directamente en un compromiso o denegación de servicio. Los escaneos internos no autorizados se consideran incidentes. La mayoría de las exploraciones externas se consideran de rutina y, caso por caso, pueden requerir respuesta e investigación.
6	Investigación	Incidentes no confirmados que son actividades potencialmente maliciosas o anómalas que la entidad informante considera que justifican una revisión adicional.

Tabla 4.2 – Categorías de incidentes

MATRIZ DE GRAVEDAD DEL INCIDENTE

Todos los incidentes de seguridad de la información deben clasificarse según el nivel de gravedad para ayudar a determinar hasta qué punto se requiere una RI formal. Los niveles de gravedad se basan en el impacto gubernamental percibido del incidente. Los niveles de gravedad pueden cambiar a medida que se desarrolla la investigación. Las definiciones generales y la descripción de cada nivel de gravedad son las siguientes:

Matriz de gravedad del incidente		
Nivel	**Definición**	**Ejemplos**
Alto	Incidentes que tienen un impacto severo en las operaciones	• Compromiso de datos sensibles • Ataque generalizado de código malicioso • Acceso no autorizado a sistemas críticos • DoS que afecta a toda la empresa
Medio	Incidentes que tienen un impacto significativo, o el potencial de tener un impacto severo, en las operaciones.	• Ataque DoS a pequeña escala • Compromisos del sitio web • Acceso no autorizado (ataques de fuerza bruta contra FTP, ssh y otros protocolos)

Bajo	Incidentes que tienen un impacto mínimo con el potencial de tener un impacto significativo o grave en las operaciones.	• Sondeos de red o análisis del sistema • Infecciones por virus aislados • Violaciones de uso aceptable

Tabla 4.3 – Matriz de gravedad del incidente

PROCEDIMIENTOS DE ESCALADA

Durante un incidente, la comunicación clara y efectiva es fundamental. Como tal, un procedimiento de escalada debe abordar todas las líneas de comunicación en caso de que ocurra un incidente. Esto incluye no sólo la comunicación interna sino también la comunicación externa. La comunicación debe fluir a través de todas las partes interesadas involucradas en RI para que todos tengan la información necesaria para actuar y llevar a cabo sus responsabilidades de manera oportuna. La notificación debe realizarse lo antes posible, pero no debe retrasar que la Repartición adopte las medidas adecuadas para aislar y contener los daños.

Cada Repartición debe tener un procedimiento de escalamiento de RI que consta de (1) una matriz de escalamiento, (2) una lista de contactos actualizada con contactos alternativos y (3) múltiples canales de comunicación, todo en un esfuerzo por garantizar que la información sea apropiada y precisa se difunde rápidamente a las partes interesadas apropiadas en RI.

ALCANCE DEL INCIDENTE

El alcance inicial lo proporciona la entidad e incluye:

- Identificar objetivos potenciales (por ejemplo, sistemas comprometidos conocidos, sistemas probablemente afectados, sistemas clave);
- Definir puntos de contacto externos (por ejemplo, Internet, conexiones inalámbricas, de terceros, de acceso remoto);
- Priorizar escenarios probables (por ejemplo, amenaza interna versus externa, ataque dirigido versus objetivo de oportunidad); y
- Visualizar el entorno dentro del alcance (por ejemplo, diagrama de red, flujo de datos).

Las consideraciones para las actividades de alcance de incidentes son las siguientes:

- Confiar en fuentes de evidencia relevantes y verificadas;

- Reducir los falsos positivos y el volumen de datos;
- Evitar un alcance excesivo y un “desplazamiento del alcance”; y
- Darse cuenta de las limitaciones operativas y de recursos puede afectar el alcance.

A medida que se desarrolla información adicional relacionada con el incidente durante el proceso de RI y a medida que se involucran más partes interesadas, un incidente generalmente requiere un nuevo alcance.

SEGUIMIENTO E INFORMES DE INCIDENTES

Un sistema de seguimiento centralizado seguro, que pueda adaptarse al acceso “necesario saber”, conduce a un esfuerzo de RI más eficiente y sistemático, además de proporcionar un seguimiento de auditoría en caso de que los esfuerzos conduzcan a un procesamiento legal de la amenaza.

Como mínimo, la documentación del incidente debe contener la siguiente información:

- Fecha/hora en que se informó el incidente
- Tipo de incidente
- Fuente de notificación del incidente
- Resumen del incidente
- Estado actual del incidente.
- Todas las acciones tomadas con respecto al incidente.
- Información de contacto de todas las partes involucradas.
- Evidencia reunida durante la investigación del incidente
- Comentarios relevantes de los miembros del equipo de RI
- Próximos pasos propuestos a seguir

Paso 3: Contención

Este paso se centra en contener la amenaza para minimizar el daño. Es durante este paso que se recopila información para determinar cómo ocurrió el ataque. Todos los sistemas afectados dentro de la Repartición deben identificarse para que la contención (y la erradicación y recuperación) sea efectiva y completa.

La contención de incidentes implica “detener la hemorragia” y evitar que el incidente se propague. La contención se puede lograr aislando los sistemas infectados, bloqueando actividades sospechosas de la red y deshabilitando servicios, entre otras acciones. La contención varía para cada incidente dependiendo de la gravedad y el riesgo de continuar con las operaciones. El liderazgo de la Repartición toma decisiones con respecto a las medidas de contención basadas en las recomendaciones del DC y/o Responsable de Seguridad.

Paso 4: Erradicación

La erradicación implica eliminar elementos de la amenaza de la red gubernamental. Las medidas de erradicación específicas dependen del tipo de incidente, la cantidad de sistemas involucrados y los tipos de sistemas operativos y aplicaciones involucradas. Las medidas típicas de erradicación incluyen volver a crear imágenes de los sistemas infectados y mejorar la supervisión de la actividad del sistema.

El análisis de la información recopilada es un proceso iterativo y ocurre o vuelve a ocurrir durante las fases de contención y erradicación.

Paso 5: Recuperación

Una vez que se ha erradicado la causa raíz de un incidente, puede comenzar la fase de recuperación. Los objetivos de este paso son: (1) remediar cualquier vulnerabilidad que contribuya al incidente (y así prevenir incidentes futuros) y (2) recuperarse restaurando las operaciones a la normalidad. A menudo se utiliza un enfoque por fases para devolver los sistemas a su funcionamiento normal, reforzarlos para evitar futuros incidentes similares y aumentar la supervisión durante un período de tiempo adecuado. Las actividades de recuperación típicas incluyen reconstruir sistemas a partir de imágenes confiables, restaurar sistemas a partir de copias de seguridad limpias y reemplazar archivos comprometidos con versiones limpias.

Se debe tener cuidado para garantizar que los archivos restaurados desde la copia de seguridad no reintroduzcan códigos maliciosos o vulnerabilidades del incidente y que el sistema esté limpio y seguro antes de volver al uso de producción. Una vez que se haya completado la recuperación, el líder de RI debe validar/certificar que el incidente se ha resuelto.

Paso 6: Aprendizaje

Un proceso de RI es tan bueno como la capacidad de ejecutarlo exitosamente. Las lecciones aprendidas pueden ser el resultado de actividades reales de RI o de pruebas de capacidad de RI, y estos resultados deben usarse para mejorar el proceso de RI identificando debilidades y deficiencias sistémicas y tomando medidas para mejorarlas. Es importante que esto tenga lugar relativamente pronto después de que se cierre el incidente.

Las lecciones aprendidas, o discusiones post mortem, proporcionan (1) un registro de los pasos tomados para responder a un ataque, (2) resultados de la investigación para determinar la causa raíz del ataque, (3) posibles mejoras a realizar, como la capacitación y certificaciones de las partes interesadas en RI,

actualizaciones de procesos y procedimientos, y modificaciones técnicas. El conocimiento adquirido se puede utilizar en un esfuerzo por prevenir y/o mitigar incidentes futuros en forma de servicios proactivos. Esto puede incluir probar el proceso de RI, realizar evaluaciones de vulnerabilidad, brindar capacitación en seguridad informática, revisar políticas y procedimientos de seguridad y difundir recordatorios de seguridad cibernética.

Tanto los informes de incidentes como los resultados de estas discusiones sobre lecciones aprendidas se colocarán en una base de datos para uso futuro y se compartirán con todas las partes interesadas de RI para el conocimiento de la situación y el desarrollo profesional.

2.3 MÉTRICAS DE RESPUESTA A INCIDENTES

Se deben compilar métricas de RI para cada incidente y reportarlas al DC y/o Encargado de Seguridad para el conocimiento de la situación gubernamental cuando sea posible y práctico.

Estas métricas permiten a las partes interesadas en RI (1) medir la efectividad de RI (y revelar posibles brechas) a lo largo del tiempo; (2) identificar tendencias en términos de actividades de amenaza y al hacerlo; (3) proporcionar justificación para recursos adicionales, para incluir personal, capacitación y herramientas adicionales.

Métricas de RI		
Categoría	**Medición**	**Descripción**
Incidentes	# Total de Incidentes / Año	Cantidad total de incidentes atendidos por año
	# Incidentes por Tipo / Año	Número total de incidentes por categoría respondidos por año
Tiempo	# Horas de Personal / Incidente	Cantidad total de mano de obra dedicada a resolver el incidente
	# Días / Incidente	Cantidad total de días dedicados a resolver el incidente
	# Horas de inactividad del sistema/Incidente	Total de horas de inactividad del sistema hasta que se resolvió el incidente

Métricas de RI		
Categoría	**Medición**	**Descripción**
Costo	Costo monetario estimado/incidente	Costo monetario total estimado por incidente, que incluye contención, erradicación y recuperación, así como actividades de recolección y análisis (esto puede incluir costos laborales, asistencia de entidades externas, adquisición de herramientas, viajes, etc.)
Daño	# Sistemas afectados / Incidente	Número total de sistemas afectados por incidente
	# Registros comprometidos / Incidente	Número total de registros comprometidos por incidente
Forense	# Total de incidentes forenses apalancados / año	Número total de incidentes que requieren análisis forense (recopilación y análisis) por año
	# Imágenes del sistema analizadas / Incidente	Número total de imágenes del sistema analizadas por incidente
	# Volcados de memoria del sistema examinados/incidente	Número total de volcados de memoria física del sistema examinados por incidente

Tabla 4.4 – Métricas de respuesta a incidentes

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 Historial de revisiones

Fecha	Descripción del cambio	Crítico