## **INSTITUTO POLITÉCNICO NACIONAL**

###### **ESCUELA SUPERIOR DE CÓMPUTO**

**IT Governance**

Profesora Jessie Paulina Guzmán Flores

Tarea 9: Escenarios NIST

**Grupo:** 3CM20 - Equipo 4

**Fecha de Entrega:** 15/Mayo/2022

**Integrantes:**

* Martínez Coronel Brayan Yosafat
* Ramírez Cotonieto Luis Fernando
* Sánchez Rojas Jesús Ubaldo

# Índice

[**Introducción**](#_t70btsdue1fh) **4**

[Análisis](#_3ar8eqvgjvua) 4

[Erradicación o Soluciones](#_tjncrztc2mbd) 4

[Post-incidente](#_7v22rqegnkuj) 4

[**Objetivos**](#_o00bt4wm3omi) **6**

[**Escenario Ataque DOS**](#_ykchfqqgta6b) **7**

[Análisis](#_gbjvh7sej35c) 7

[Erradicación](#_jy2e15grlibe) 7

[Post-incidente](#_hxj9y828fq67) 8

[**Escenario PC infectada**](#_rz5e83jpaj33) **8**

[Análisis](#_gdjzzlwplcm1) 8

[Erradicación](#_9shxj28orame) 9

[Post-incidente](#_u8smfbx4v1nh) 9

[**Escenario Rootkit**](#_trx93ec9j4px) **9**

[Análisis](#_v9sy7gilstv2) 10

[Erradicación](#_aca9s8j8dfd2) 10

[Post-incidente](#_wvnqixsruui4) 10

[**Escenario DB comprometida**](#_vje0yftdaxcg) **10**

[Análisis](#_bijnmdpo5snd) 11

[Erradicación](#_4y3758ounsjp) 11

[Post-incidente](#_m7g2dxcn8ftx) 11

[**Escenario Acceso desconocido**](#_oiwjlnie05r) **11**

[Análisis](#_gpdtamjfql0c) 12

[Erradicación](#_qssrgwj5acb6) 12

[Post-incidente](#_4rmg5odafraa) 12

[**Referencias**](#_z0jfgnvimn9n) **13**

# Introducción

En la vida de los encargados de la información se presentarán diversas situaciones a las que deberán tomar decisiones de una forma inmediata para su solución, podemos encontrar las siguientes áreas en las que se deberá realizar diversas preguntas:

## Análisis

* ¿Consideraría la empresa la situación como un incidente?, si lo hiciera, ¿qué políticas o normas violaría la situación?
* ¿Qué medidas ya existen para prevenir este tipo de incidente?
* ¿Qué precursores se han detectado de este incidente?, ¿Alguno de ellos haría que la empresa tome cartas en el asunto?
* ¿Qué indicadores podríamos detectar?, ¿Cuáles podrían causar que alguien piense que el incidente ya ha ocurrido?
* ¿Qué herramientas adicionales podrían ser necesarias para la detección de este incidente?
* ¿Cómo respondería el equipo para analizar y validar este incidente?
* ¿Qué personal estaría involucrado en este análisis y validación?
* ¿Para qué personas y grupos el equipo reportará el incidente?
* ¿Cómo priorizaría el incidente el equipo?

## Erradicación o Soluciones

* ¿Qué estrategia debería tomar la organización para contenerlo?, ¿Por qué esa y no otra?
* ¿Qué pasaría si el incidente no es controlado?
* ¿Qué personal estará involucrado con la erradicación, recuperación y/o contención del incidente?
* ¿Qué fuentes de evidencia (si hay) deberían de mantenerse?, ¿Cómo será adquirida esta evidencia?, ¿Por cuánto tiempo?, ¿Dónde estará alojada?

## Post-incidente

* ¿Quién atendería las sesión de lecciones aprendidas con este incidente?
* ¿Qué podría haberse hecho para prevenir incidentes similares?
* ¿Qué podría hacerse para mejorar la detección de incidentes similares?
* ¿Cuál será la futura estrategia a tomar?
* ¿Qué otras direcciones deberían ser consideradas como un riesgo mayor?

Preguntas generales

* ¿Cuánta gente y organizaciones han sido involucradas en este incidente?
* ¿A qué partes externas va a reportar el equipo?, ¿Cuándo se harán estos reportes?, ¿Cómo se harán?, ¿Qué información se va a reportar y cuál no?, y, ¿Por qué esa información?
* ¿Cuáles medidas se tomarán para este reporte?
* ¿Qué otras comunicaciones externas podrían ocurrir?
* ¿Qué herramientas y recursos debería de tener el equipo para el manejo de este incidente?
* ¿Qué aspectos del manejo deberían haber sido diferentes si hubiera ocurrido en una hora diferente?
* ¿Qué aspectos cambiarían si hubiera ocurrido en otra ubicación?

# Objetivos

* Leer el material anexo de la actividad.
* Resolver los incidentes alineados al NIST, esto significa considerar las fases y las acciones se tomaron (mínimo 3 casos que puede tomar cada escenario).

Tomando en cuenta:

* daño colateral
* variantes de cada solución ( detallados)
* variantes del incidente
* restricciones y alcance de cada solución planteada

# Escenario Ataque DOS

Un sábado por la tarde, los usuarios externos empiezan a tener problemas para acceder a los sitios web públicos de la organización. Durante la siguiente hora, el problema se agrava hasta el punto de que casi todos los intentos de acceso fallan. Mientras tanto, un miembro del personal de redes de la organización responde a las alertas de un router de frontera de Internet y determina que el ancho de banda de Internet de la organización está siendo consumido por un volumen inusualmente grande de paquetes del Protocolo de Datagramas de Usuario (UDP) hacia y desde los dos servidores públicos de DNS de la organización. El análisis del tráfico muestra que los servidores DNS están recibiendo grandes volúmenes de peticiones desde una única dirección IP externa. Además, todas las solicitudes de DNS de esa dirección provienen del mismo puerto de origen.

## Análisis

* ¿Qué precursores del incidente, si los hay, podría detectar la organización? Respuesta: (por ejemplo, aumento de las llamadas al centro de llamadas y al servicio de asistencia informática, notificación del MSP)
* ¿Algún precursor haría que la organización tomara medidas antes de que se produjera el incidente? Respuesta: (Por ejemplo, no es probable, el impacto casi en tiempo real de los ataques DDOS significa que cualquier de los clientes/miembros o las alertas generadas por el sistema indicarían que el ataque ya estaba en marcha).
* ¿Qué herramientas adicionales podrían ser necesarias para detectar este incidente en particular? Respuesta: (por ejemplo, monitorización/alerta de terceros. Para internos; herramientas de monitorización de la red).
* ¿Cómo analizará y validará este incidente el equipo de respuesta a incidentes? ¿Qué personal participa en el proceso de análisis y validación? Respuesta: (por ejemplo, terceras partes como Network Solutions, Network Carrier (ATT), MSSP, Ingeniero de redes).
* ¿A qué personas y grupos de la organización informará el equipo del incidente? Respuesta: (por ejemplo, CIRT, dirección superior, auditoría interna, grupos de intercambio de información: FS-ISAC)
* ¿Cómo priorizaría el equipo la gestión de este incidente? Respuesta: (por ejemplo, la comunicación a los clientes/miembros, los sistemas críticos de producción se de producción)

## Erradicación

* ¿Qué estrategia debe adoptar la organización para contener el incidente? ¿Por qué es preferible esta estrategia a otras? Respuesta: (por ejemplo, la comunicación a los clientes/miembros y a los proveedores de terceros será prioritaria para minimizar el daño a la reputación)
* ¿Qué podría ocurrir si no se contuviera el incidente? Respuesta: (por ejemplo, daño a la reputación, impacto financiero)
* ¿Qué herramientas adicionales podrían ser necesarias para responder a este incidente en particular? Respuesta: (por ejemplo, servicios de respuesta a incidentes de un proveedor externo para ayudar en el proceso de recogida de pruebas forenses, FBI)

## Post-incidente

* ¿Cómo se captarán las lecciones aprendidas? Se realizarán estadísticas con los recursos que se pudieron haber perjudicado y los gastos ahorrados por tener al equipo de seguridad
* ¿Quiénes estarán en las lecciones aprendidas? Especialmente las personas que no saben cómo funciona la seguridad informática.

# Escenario PC infectada

Un martes por la mañana, se libera un nuevo gusano; se propaga a través de medios extraíbles y puede copiarse a sí mismo en los recursos compartidos de Windows. Cuando el gusano infecta un host, instala un agente DDoS. La organización ya ha incurrido en infecciones generalizadas antes de que las firmas antivirus estén disponibles varias horas después de que el gusano comienza a propagarse.

## Análisis

* ¿Qué fuentes de pruebas, si las hay, debería adquirir la organización? ¿Cómo se adquirirán las pruebas? ¿Dónde se almacenarán? ¿Durante cuánto tiempo deberían conservarse? Respuesta: (Por ejemplo, se recopilarán y almacenarán fuera de línea 30 días de datos de registro de los servidores/ordenadores personales/aplicaciones. La recogida de pruebas será realizada por un proveedor de pruebas forenses contratado para garantizar las mejores práctica)
* ¿Cómo podría el equipo de respuesta a incidentes identificar todos los hosts infectados? Respuesta: (por ejemplo, los sistemas de gestión de activos y de gestión de parches están en marcha y se utilizarán para asegurar que todos los hosts de la red sean escaneados)
* ¿Cómo intentaría la organización evitar que el gusano se propagara por los hosts infectados antes de que se publicaran las firmas antivirus? ¿antes de que se publiquen las firmas antivirus? Respuesta: (por ejemplo, la segmentación de la red, los puertos compartidos de Windows se bloquearán para impedir temporalmente la propagación de la infección)
* ¿Intentará la organización parchear todos los equipos vulnerables? En caso afirmativo, ¿cómo se haría? Respuesta: (Por ejemplo, sí, las máquinas vulnerables se parchearon a través del sistema de gestión de parches y seguirán los procedimientos de gestión de parches actualmente en vigor).

## Erradicación

* ¿Cómo cambiaría la gestión de este incidente si los hosts infectados que habían recibido el agente DDoS hubieran se hubieran configurado para atacar el sitio web de otra organización a la mañana siguiente? Respuesta: (por ejemplo, la priorización cambiaría para incluir la notificación a la otra organización y implementación de reglas de firewall para evitar la comunicación en la red)
* ¿Cómo cambiaría la gestión de este incidente si uno o varios de los hosts infectados contuviera información sensible información personal identificable de los empleados de la organización? Respuesta: (Por ejemplo, la notificación a los empleados de la posible exposición de información personal sería gestionada por el departamento de RRHH).
* ¿Cómo mantendrá el equipo de respuesta a incidentes a los usuarios de la organización informados sobre el estado del incidente? Respuesta: (por ejemplo, la organización seguirá el procedimiento de comunicación del PBC para seguir informando a los empleados afectados)

## Post-incidente

* ¿Qué medidas adicionales llevaría a cabo el equipo para los hosts que no están actualmente conectados a la red (por ejemplo, los miembros del personal que están de vacaciones, los empleados fuera de la sede que se conectan ocasionalmente)? Respuesta: (por ejemplo, comunicaciones de TI/HR, así como el bloqueo de la conexión de los teletrabajadores remotos hasta que se hayan verificado los parches)

# Escenario Rootkit

Un lunes por la mañana, la organización recibe una llamada de la Oficina Federal de Investigación (FBI) sobre una actividad sospechosa en los sistemas de la organización. Ese mismo día, un agente del FBI se reúne con miembros de la dirección y del departamento jurídico para hablar de la actividad. El FBI ha estado investigando actividades relacionadas con la publicación de documentos sensibles, y algunos de los documentos pertenecen a la organización. El agente solicita la ayuda de la organización y la dirección de la organización, solicita la ayuda del equipo de respuesta a incidentes para adquirir las pruebas necesarias para determinar si estos documentos son legítimos o no y cómo podrían haberse filtrado.

## Análisis

* ¿Qué políticas e incluso leyes violaría un incidente de este tipo?
* ¿Cuáles serían los motivos si es una persona interna? Podrían ser por insatisfacción, habría que tener un área encargada de que no suceda.
* ¿Qué procesos tuvo que pasar para que esa persona tuviera ese puesto?

## Erradicación

* ¿De qué fuentes podría el equipo de respuesta a incidentes reunir pruebas? Respuesta: (por ejemplo, registros de gestión de cambios, registros de vigilancia, registros de controles de acceso, registros de DLP)
* ¿Qué haría el equipo para mantener la confidencialidad de la investigación? Respuesta: (por ejemplo, limitar el número de miembros del IRT involucrados)
* ¿Cómo cambiaría la gestión de este incidente si el equipo identificará a un anfitrión interno responsable de las filtraciones? Respuesta: (es decir, se retiraría/se pondría en cuarentena al anfitrión interno en busca de pruebas y se compartiría con el FBI)
* ¿Cómo cambiaría la gestión de este incidente si el equipo encontrará un rootkit instalado en el host interno responsable de las filtraciones? Respuesta: (por ejemplo, se comprobarán todos los sistemas en busca del rootkit identificado)

## Post-incidente

* ¿Qué políticas nuevas se deberían de implementar?
* ¿Deberíamos de cambiar los permisos de los roles, o incluso, revisar todos los que tenemos?

# Escenario DB comprometida

Un martes por la noche, un administrador de bases de datos realiza un mantenimiento fuera de horario en varios servidores de bases de datos de producción. El administrador se da cuenta de que hay algunos nombres de directorios desconocidos e inusuales en uno de los servidores. Después de revisar los listados de directorios y ver algunos de los archivos, el administrador concluye que el servidor ha sido atacado y llama al equipo de respuesta a incidentes para pedir ayuda. La investigación del equipo determina que el atacante consiguió acceso de root al servidor hace seis semanas.

## Análisis

* ¿Qué fuentes podría utilizar el equipo para determinar cuándo se ha producido el compromiso? Respuesta: (por ejemplo, registros SIEM, registros MSSP, tickets de gestión de cambios)
* ¿Se debería sospechar desde un inicio que fuera alguien del equipo interno?

## Erradicación

* ¿Cómo cambiaría la gestión de este incidente si el equipo descubriera que el servidor de la base de datos ha estado que el servidor de la base de datos había estado ejecutando un sniffer de paquetes y capturando contraseñas de la red? Respuesta: (Por ejemplo, se cambiarían las contraseñas de las cuentas administrativas y no cambiadas para todos los empleados).
* ¿Cómo cambiaría la gestión de este incidente si el equipo descubriera que el servidor estaba ejecutando un proceso que copiaba una base de datos que contenía información sensible de los clientes (incluida la información identificable) cada noche y la transfiere a una dirección externa? Respuesta: (por ejemplo, notificar a las autoridades apropiadas, es decir, al FBI, a la policía local de la posible exposición de PII, notificar a los empleados afectados de la posible exposición)
* ¿Cómo cambiaría la gestión de este incidente si el equipo descubriera un rootkit en el servidor? Respuesta: (Por ejemplo, el servidor se retiraría del entorno de producción para la recogida de pruebas forenses. Se escanearon todos los servidores en busca del rootkit identificado. Se ejecutaría el proceso BCP para servidor afectado).

## Post-incidente

* ¿Qué acciones vamos a comunicar ante nuestros clientes?
* ¿Daremos alguna compensación por lo sucedido?
* ¿Qué procesos vamos a implementar para evitar esto?

# Escenario Acceso desconocido

Un lunes por la mañana, el servicio de asistencia de la organización recibe llamadas de tres usuarios de la misma planta de un edificio que afirman tener problemas con su acceso inalámbrico. Un administrador de red al que se le pide que ayude a resolver el problema lleva un portátil con acceso inalámbrico a la planta de los usuarios. Mientras ve su configuración de red inalámbrica, se da cuenta de que hay un nuevo punto de acceso que aparece como disponible. Comprueba con sus compañeros de equipo y determina que este punto de acceso no fue desplegado por su equipo, por lo que lo más probable es que se trate de un punto de acceso fraudulento que se ha establecido sin permiso.

## Análisis

* ¿Cuál debería ser el primer paso importante en la gestión de este incidente (por ejemplo, encontrar físicamente el punto de acceso fraudulento, conectarse lógicamente al punto de acceso)? Respuesta: (Por ejemplo, localizar físicamente el dispositivo, se revisarán los registros de control de acceso a la red (NAC). Se revisarán los registros de cambio de los puertos habilitados/deshabilitados para identificar la ubicación del rogue)

## Erradicación

* ¿Cuál es la forma más rápida de localizar el punto de acceso? ¿Cuál es la forma más oculta de localizar el punto de acceso? Respuesta: (Escanear la red en busca de dispositivos falsos)
* ¿Cómo se manejaría este incidente si el punto de acceso hubiera sido desplegado por una parte externa (por ejemplo, un contratista) que trabaja temporalmente en la oficina de la organización? Respuesta: (por ejemplo, contactar con el propietario del contrato y el proveedor o proveedores. Revisar los documentos de aprobación para la instalación del dispositivo inalámbrico, Identificar las lagunas en el proceso de gestión del proveedor)
* ¿Cómo sería la gestión de este incidente si un analista de detección de intrusos informara de signos de actividad sospechosa en algunos de los puestos de trabajo de la misma planta del edificio? Respuesta: (por ejemplo, el alcance de la respuesta al incidente se ampliará para incluir el escaneo de las estaciones de trabajo en la misma planta, así como los servidores/aplicaciones accesibles desde los puestos de trabajo)
* ¿Cómo sería la gestión de este incidente si el punto de acceso hubiera sido retirado mientras el equipo? ¿Intenta el equipo localizarlo físicamente? Respuesta: (Pruebas forenses (se revisarán/conservarán los registros para identificar el punto de entrada)

## Post-incidente

* ¿Deberíamos investigar si existen más accesos desconocidos?
* ¿Se accedió a información crítica para la empresa?
* Si sí, ¿cómo vamos a responder ante las autoridades y nuestros clientes?

# Referencias

Ciberseguridad Marco NIST, Un abordaje integral de la Ciberseguridad: <https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf>

MARCO DE PRIVACIDAD DEL NIST: UNA HERRAMIENTA PARA MEJORAR LA PRIVACIDAD POR MEDIO DE LA GESTIÓN DE RIESGOS EMPRESARIALES, VERSIÓN 1.0 : <https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932988>

Incident Response Scenarios Playbook: <https://www.blackswantechnologies.com/wp-content/uploads/2019/03/Black-Swan-Technologies-Incident-Response-Scenarios-Playbook-2019.pdf>