Gestión de Incidentes de Ciberseguridad

Jornada Nacional de Ciberseguridad

Cómo prepararnos, responder y aprender de los incidentes que marcan el panorama digital actual.

Equipo de Respuesta a Incidentes de Seguridad Informática de BCF, CSIRT

Empresa de Tecnologías de la información

eti
Tecnologías de la Información BioCubaFarma

¿Qué es la Gestión de Incidentes?

La Gestión de Incidentes es el proceso que se realiza con el objetivo de prevenir, detectar y enfrentar los incidentes de Ciberseguridad y comprende las acciones que se realizan antes, durante y después de su ocurrencia. (Decreto 360 “Sobre La Seguridad De Las Tecnologías De La Información Y La Comunicación Y La Defensa Del Ciberespacio Nacional”) (GOC-2019-O45)

En Cuba, este proceso está regulado por la Resolución 105 “Reglamento Sobre El Modelo De Actuación Nacional Para La Respuesta A Incidentes De Ciberseguridad”, que define cuatro etapas esenciales para su correcta ejecución. A estas etapas se añade la fase de “Lecciones Aprendidas”, donde se evalúa lo ocurrido y se identifican mejoras para fortalecer la respuesta en el futuro.

Prevención y Protección

Detección, Evaluación y Notificación

Investigación

Mitigación y Recuperación

Lecciones Aprendidas

Detección Proactiva

Las organizaciones necesitan un enfoque proactivo, capaz de detectar señales tempranas, comportamientos anómalos y actividades sospechosas *antes* de que se conviertan en un problema mayor. La detección en tiempo real es, hoy, uno de los pilares que define si un ataque será apenas un susto… o un evento de alto impacto.

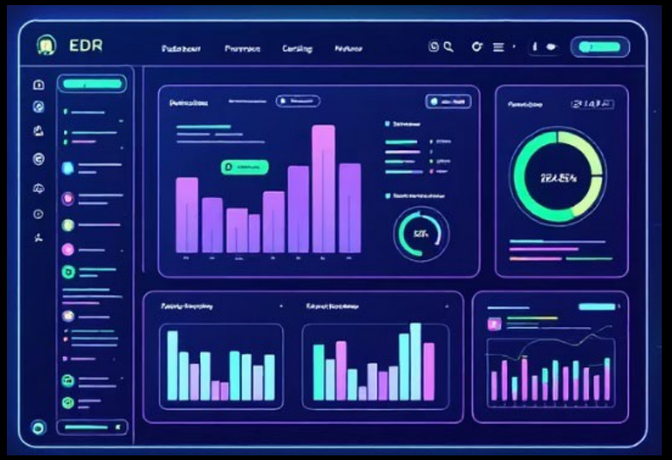
La detección en tiempo real permite:

- Identificar actividades sospechosas antes de que se conviertan en incidentes mayores.
- Reducir el impacto financiero y operativo.
- Detectar campañas avanzadas (APT) que se esconden durante meses.
- Prevenir fugas de información sensible.

Técnicas de Detección Proactiva

Para lograr una detección temprana y efectiva, las organizaciones necesitan apoyarse en tecnologías capaces de identificar anomalías, correlacionar eventos y anticipar comportamientos maliciosos. Estas son algunas de las herramientas y técnicas más utilizadas para detectar incidentes a tiempo y mantener una vigilancia continua sobre el entorno digital.

- Sistemas SIEM con correlación de eventos
- Sistemas de detección y prevención de intrusiones (IDS/IPS)
- Monitoreo de endpoints (EDR/XDR)
- Threat hunting
- Inteligencia de amenazas
- Análisis de comportamiento del usuario (UEBA)



La criticidad del tiempo

Cuando ocurre un incidente de ciberseguridad, el tiempo se convierte en un recurso crítico. Cada minuto que pasa sin una respuesta adecuada puede aumentar el impacto económico, operativo y reputacional del ataque.

Una respuesta temprana no solo reduce los riesgos, sino que también contribuye a mantener la continuidad del negocio y cumplir con las exigencias regulatorias que rigen la gestión de incidentes.

Propagación del ataque a sistemas y datos críticos.

Pérdida masiva de datos o un impacto económico mayor.

Interrupción prolongada de servicios esenciales.

Sanciones por incumplimiento de plazos regulatorios.

Mayor tiempo de recuperación elevando significativamente los costos.

Daño a la imagen corporativa y pérdida de confianza.

Top 5 de Amenazas Críticas

1 Infección por malware

Software malicioso que pueden propagarse, robar información o conectarse a servidores externos. Los casos incluyen RETADUP, SINKHOLE, botnets como MyKings, BADBOX, HotRat y campañas como This Spider Bytes Like Ice.

2 Escaneos y reconocimiento

Búsqueda automatizada de puertos y servicios para detectar vulnerabilidades o equipos comprometidos. Incluyen escaneos SSH, RDP y escaneo a puertos como 3306 y 445.

3 Uso indebido de red

Actividades de usuarios que usan la red para fines no permitidos. Incluye casos como el empleo de redes P2P, uso masivo de redes TOR y consultas DNS a sitios indebidos.

4 Correo no deseado (SPAM)

Envío o recepción masiva de correos no solicitados, generalmente desde cuentas comprometidas.

5 Explotación de vulnerabilidades

Intentos de aprovechar fallos en sistemas internos o expuestos, generalmente para obtener control remoto o ejecutar código.

Exposición en Redes de Datos móviles

Las redes móviles modernas combinan múltiples tecnologías y servicios, lo que las convierte en un entorno tan flexible como vulnerable. La evolución hacia 4G/5G, la coexistencia con protocolos antiguos y la creciente dependencia de dispositivos IoT amplían la superficie de ataque y exponen nuevos vectores que los atacantes pueden explotar.

Riesgos en la cadena de suministro

La interconexión entre operadores y proveedores introduce vulnerabilidades externas difíciles de controlar.

Explotación de IoT móvil

Dispositivos mal asegurados pueden ser comprometidos o utilizados como puerta de entrada.

Protocolos heredados vulnerables

La presencia de 2G/3G permite ataques de interceptación y rastreo de dispositivos.

Ataques a la señalización y estaciones base

Suplantación de antenas (IMSI catchers), manipulación de señalización y denegación de servicio.

Riesgos por virtualización (NFV/SDN)

Configuraciones débiles en redes basadas en software abren nuevas oportunidades para intrusiones.

Seguridad en redes LAN

Aunque gran parte de la atención se centra en amenazas externas y remotas, la red LAN sigue siendo el corazón de la infraestructura corporativa. Es el espacio donde se conectan servidores, estaciones de trabajo, impresoras, cámaras IP y dispositivos críticos.

Una LAN mal configurada se convierte en un escenario perfecto para movimientos laterales, escalamiento de privilegios y ataques internos,

Fortalecer la red LAN es uno de los pasos más efectivos para evitar que un incidente aislado se convierta en un compromiso masivo.

Segmentación de red

Dividir la red para limitar movimientos laterales y reducir el impacto de un incidente.

Control estricto de accesos

Aplicar el mínimo privilegio para evitar accesos indebidos y abuso de permisos.

Actualización de equipos

Mantener switches y routers al día para evitar vulnerabilidades críticas.

Implementación de IDS/IPS

Detectar y bloquear tráfico malicioso antes de que afecte la red interna.

Desactivación de puertos

Deshabilitar o proteger puertos físicos no usados.