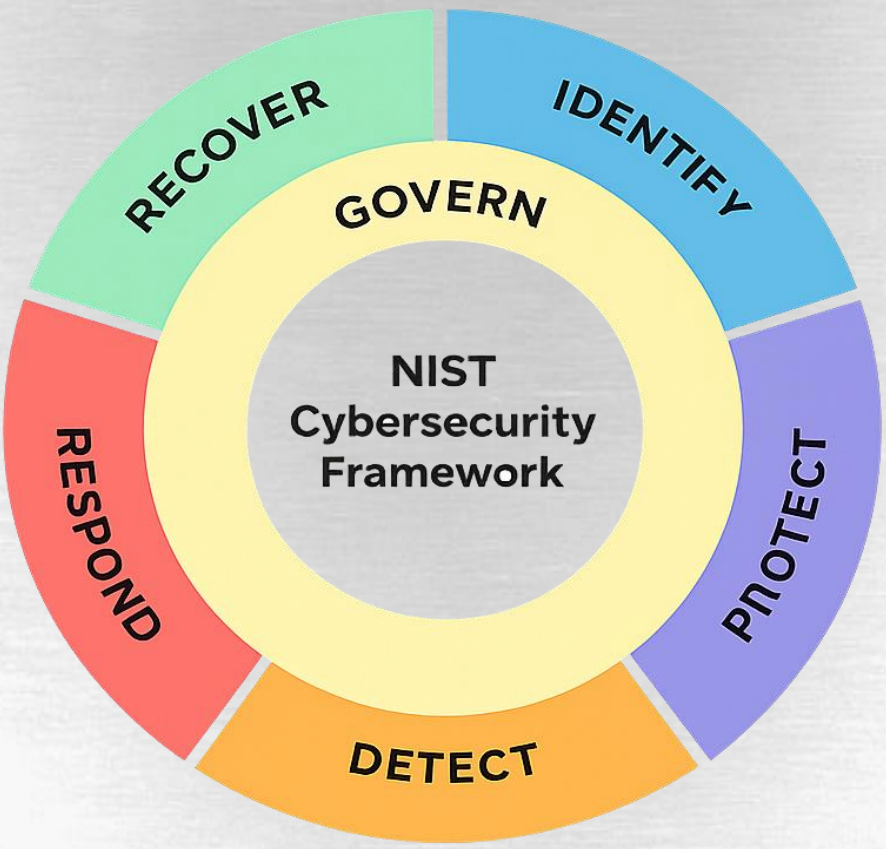
(NIST, DOJ, DHS, CISA)

Plan de Respuesta a Incidentes

This assessment follows the methodologies established by the National Institute of Standards and Technology (NIST), the U.S. Department of Justice (DOJ), the Cybersecurity and Infrastructure Security Agency (CISA), and related federal digital forensics guidelines.

4Geeks Academy

ERIC GROSSERMANN
Digital Examiner



Respuesta a Incidentes y (SGSI) ISO 27001

Fecha De Entrega: 01/09/26

GROSSERMANN
PENTESTER
CYBER SECURITY

Introduccion

En esta Fase 3 del proyecto final desarrollado en 4Geeks Academy, se diseña un Plan de Respuesta a Incidentes basado en las mejores prácticas de la industria, tomando como referencia los lineamientos del NIST y su guía SP 800-61, así como el marco de funciones del NIST Cybersecurity Framework (CSF). El objetivo principal de esta fase es establecer un enfoque estructurado y técnico para la gestión de incidentes de seguridad que afecten a servidores críticos de la organización.

El plan propuesto describe de manera detallada cómo la organización identifica, protege, detecta, responde y se recupera de incidentes de seguridad similares al hackeo previamente analizado. Asimismo, esta fase integra controles preventivos y correctivos alineados con un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001, incorporando mecanismos de protección de datos, controles de acceso, monitoreo continuo y procedimientos de mejora continua, con el fin de reducir el impacto de futuros incidentes y prevenir su recurrencia.

Annex A

IDentificacion

Durante la fase de Identificación, el analista de ciberseguridad investigó un evento de seguridad que afectó a un servidor crítico dentro de la infraestructura simulada de 4Geeks Academy. El incidente fue identificado mediante el análisis de registros del sistema y de servicios, donde se evidenciaron configuraciones inseguras y servicios innecesariamente expuestos, incrementando la superficie de ataque del servidor.

Relevancia para la Seguridad de la Información

El análisis forense inicial incluyó la revisión de archivos de logs del sistema operativo y servicios críticos, tales como registros de autenticación, servicios web y base de datos. A través de esta revisión se detectaron intentos de acceso no autorizados, así como la presencia de servicios activos sin una justificación operativa clara, lo cual permitió inferir que el atacante aprovechó fallos de configuración y falta de controles preventivos para comprometer el sistema.

Como resultado de esta fase, se determinó que la causa raíz del incidente estuvo relacionada con deficiencias en la configuración de seguridad, ausencia de un monitoreo centralizado efectivo y falta de controles formales de gestión de riesgos. Estos hallazgos confirmaron la necesidad de aplicar medidas de protección, detección y respuesta estructuradas, alineadas con las mejores prácticas del NIST Cybersecurity Framework y como base para el desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a ISO/IEC 27001.

Annex B

Protección

Para reducir el riesgo de recurrencia asociado a accesos no autorizados por SSH, se implementaron controles preventivos (hardening) enfocados en reducir superficie de ataque y endurecer autenticación. En primer lugar, se restringió el acceso a SSH mediante reglas de firewall, permitiendo únicamente conexiones desde IPs autorizadas o redes administrativas (whitelisting) y limitando exposición innecesaria del puerto. Adicionalmente, se reforzó la configuración del servicio SSH deshabilitando autenticación por contraseña en favor de llaves, bloqueando acceso directo del usuario root, y reduciendo vectores comunes de fuerza bruta mediante parámetros de seguridad (p. ej., límites de intentos y tiempos de espera).

Como control complementario, se incorporó un mecanismo automático de mitigación de fuerza bruta como Fail2ban, que analiza registros de autenticación y bloquea IPs con múltiples intentos fallidos. Finalmente, se definieron políticas básicas de gestión de credenciales y mínimo privilegio para evitar que credenciales comprometidas permitan escalamiento o persistencia.

Nota de alineación a industria (opcional): En un entorno corporativo, estas medidas se pueden fortalecer con reglas analíticas en un SIEM (por ejemplo, Microsoft Sentinel) para endurecer y automatizar controles; sin embargo, los controles aplicados aquí son plenamente válidos y realistas para un entorno junior/on-premise.

Annex C

Detección

Para mejorar la capacidad de detección ante intentos de intrusión por SSH, se estableció un enfoque de monitoreo basado en logs y correlación. Se habilitó el registro detallado de eventos de autenticación y se definieron patrones de detección sobre señales típicas de ataque, incluyendo: múltiples fallos de login, intentos de acceso a usuarios inexistentes, cambios repentinos en frecuencia de conexiones, accesos fuera de horarios normales y autenticaciones exitosas desde ubicaciones/IPs no habituales.

Como mecanismo central, se implementó monitoreo y alertamiento mediante un sistema tipo Wazuh/SIEM, permitiendo generar alertas ante:

- Login exitoso sospechoso (éxito después de múltiples fallos)
- Uso de cuentas privilegiadas o intentos de sudo
- Cambios en archivos sensibles relacionados con acceso (p. ej., sshd_config, authorized_keys)

Este esquema aumenta visibilidad y reduce el tiempo de detección (MTTD), permitiendo actuar antes de que el atacante consolide acceso o persistencia.

Annex D

Respuesta

Ante la detección de actividad anómala o confirmación de compromiso por SSH, el equipo de respuesta ejecuta un procedimiento de contención y análisis. Primero, se bloquean las IPs ofensivas mediante firewall y/o Fail2ban, y se limita temporalmente el acceso remoto mientras se preserva evidencia. Luego se revisan logs para confirmar alcance del incidente (cuentas afectadas, comandos ejecutados, escalamiento, persistencia) y se identifican indicadores de compromiso (IoCs).

Posteriormente se aplican acciones inmediatas:

- ➔ Rotación de credenciales y revisión de llaves SSH
- ➔ Validación de integridad de cuentas y permisos (usuarios/sudoers)
- ➔ Parcheo/configuración segura del vector explotado
- ➔ Documentación técnica del incidente (línea de tiempo, evidencias, acciones)

Si existiera un SIEM como Sentinel (opcional): Se podría configurar un playbook de respuesta (SOAR) que automatice tareas como bloquear IPs, abrir ticket, notificar al equipo, aislar el host y recolectar evidencias. En este proyecto, la respuesta se mantiene realista a un entorno local: bloqueo, contención, análisis y remediación documentada.

Annex E

Recuperación

Durante la recuperación, el objetivo es restablecer operación segura con mínima interrupción del servicio.
El sistema se devuelve a un estado confiable mediante validación de integridad, verificación de servicios críticos y revisión de configuraciones endurecidas.
En caso de corrupción o duda razonable, se procede a restauración desde respaldos verificados (backups), asegurando que el punto de restauración no contenga compromiso.

Para mantener continuidad del negocio, se definen medidas como:

- ➢ Acceso administrativo restringido y monitoreado
- ➢ Procedimientos de restauración
- ➢ Monitoreo intensivo post-incidente (72 horas o ventana definida)

- Revisión y actualización del playbook

Finalmente, se revisan métricas operativas (tiempo de recuperación y efectividad de controles) para mejorar la capacidad de respuesta futura y reducir el impacto en caso de nuevos intentos de intrusión por SSH.

Lecciones Aprendidas Post-Incidente

Detección y análisis efectivos: El monitoreo de registros de autenticación permitió identificar patrones anómalos asociados a intentos de acceso no autorizado por SSH, confirmando la utilidad de los mecanismos de logging y revisión de eventos.

Confirmación del incidente (True Positive): El análisis forense validó que los eventos detectados correspondían a actividad maliciosa real, demostrando la fiabilidad del enfoque de detección basado en logs y correlación.

Contención oportuna: La aplicación de controles como bloqueo de IPs, endurecimiento de SSH y mitigación de fuerza bruta redujo el impacto del incidente y evitó su escalamiento.

Documentación y aprendizaje: El incidente fue documentado adecuadamente, permitiendo mejorar procedimientos y fortalecer la preparación ante eventos similares.

Áreas de Mejora

Mejorar detección y correlación: Ampliar reglas de detección para identificar comportamientos más complejos (por ejemplo, accesos exitosos tras múltiples fallos o patrones de “low and slow”) y enriquecer alertas con contexto adicional.

Automatización de la respuesta: Incorporar mayor automatización en acciones de respuesta (bloqueo automático de IPs persistentes, alertas priorizadas, flujos de notificación) para reducir tiempos de reacción y dependencia manual.

Estandarización de playbooks: Formalizar y versionar playbooks de respuesta para SSH y accesos remotos, asegurando consistencia operativa y mejora continua.

Mejoras Continuas Recomendadas

El fortalecimiento continuo del entorno —incluyendo hardening de servicios, monitoreo centralizado, políticas de acceso y pruebas periódicas— permitirá mitigar ataques similares en el futuro. La adopción gradual de prácticas alineadas con un SGSI conforme a ISO/IEC 27001, junto con procedimientos de respuesta basados en NIST, incrementará la resiliencia operativa y reducirá el riesgo residual ante incidentes de seguridad.