

TECNICATURA UNIVERSITARIA EN CIBERSEGURIDAD

**SISTEMAS DE GESTIÓN DE SEGURIDAD
DE LA INFORMACIÓN (MARCOS
NORMATIVOS)**

Ejercicio integrador simulador-optativo
**Universidad del
Gran Rosario**

**Profesor: Lic. Juan Pablo Villalba
Tec. Tomás Navarro**

**Alumno: Balbuena Atar Dante Gabriel
Tucumán, Tafí Viejo – noviembre 2024**

1. Introducción

2. Desarrollo

- Paso 1: Respuesta Inmediata al Ciberataque
 - Identificación del Incidente
 - Informe de Detección Temprana
 - Contención y Mitigación del Incidente
- Paso 2: Recuperación y Resiliencia
 - Restauración de Sistemas Críticos
 - Infraestructura VMware
 - Control de Acceso y Monitoreo
 - Informe de Mejora Continua
- Paso 3: Gestión del Incidente con Terceras Partes
 - Evaluación y Gestión de Proveedores
 - Compromiso con Pruebas de Seguridad
 - Auditoría de Seguridad
- Paso 4: Ejercicio de Resiliencia del NIST 2.0
 - Simulación de Ciberataque y Evaluación
 - Fase de Detección
 - Fase de Respuesta Inmediata
 - Fase de Recuperación
 - Métricas de Evaluación
- Paso 5: Redacción de Formularios y Políticas de Cumplimiento
 - Formulario de Consentimiento de Clientes (GDPR)
 - Política Interna de Gestión de Ciberincidentes
 - Acuerdo de Nivel de Servicio (SLA) para Proveedores

3. Conclusiones

4. Anexo

5. Referencias

1. INTRODUCCION



La creciente importancia de la ciberseguridad responde al incremento de ciberataques en empresas, especialmente en el sector del comercio electrónico. En este ejercicio, se hará un ataque simulado contra EcoShop, una tienda en línea que ha sido blanco de un ataque de ransomware. Este ataque se originó a partir de una campaña de phishing que aprovechó una vulnerabilidad no parcheada en la infraestructura de VMware de la empresa. El ataque interrumpió la plataforma de ventas y comprometió la seguridad de los datos de los clientes. En el presente informe se detallan las acciones que se deberán tomar para responder a este incidente, los pasos para la recuperación de sistemas críticos y las estrategias para reforzar la resiliencia de la organización frente a futuros ataques. Para ello, se aplicarán estándares y normativas internacionales y locales, como los lineamientos del NIST CSF 2.0, la ISO 27001, el GDPR y las disposiciones del BCRA, asegurando un enfoque integral en la gestión de ciberincidentes y la protección de datos.

2. DESARROLLO

Paso 1: Respuesta Inmediata al Ciberataque

1. Identificación del Incidente

EcoShop sufrió un ataque de ransomware que se originó a través de un correo electrónico de phishing, el cual permitió el acceso indebido a su infraestructura de virtualización y provocó la interrupción de su plataforma de ventas. Como parte del **Análisis Forense Inicial**, se utilizaron herramientas EDR (Detección y Respuesta en el Endpoint) y SIEM (Gestión de Eventos e Información de Seguridad) para rastrear el punto de entrada del ataque y cómo se propagó el ransomware.

Informe de Detección Temprana

Siguiendo las pautas de la función de **Detección** del NIST CSF, se elaboró un informe con los siguientes detalles:

Elemento	Descripción
Tiempo de detección	Aproximadamente 20 minutos tras la detección de actividad inusual.
Métodos de identificación	SIEM detectó patrones irregulares, y el EDR alertó intentos de modificar configuraciones.
Activos comprometidos	Servidor de virtualización, sistema de ventas en línea y estaciones de trabajo en red.
Vulnerabilidades	Explotación de vulnerabilidad en VMware, habilitada por phishing.

2. Contención y Mitigación del Incidente

Para frenar la propagación del ransomware y reducir su impacto en la infraestructura de EcoShop, se sugiere el siguiente plan de contención y mitigación, de acuerdo con la comunicación "A" 7266 del BCRA.

Aislamiento de Sistemas

Es fundamental aislar de inmediato los sistemas que han sido afectados y aquellos en riesgo de infección. Esto incluye el servidor de virtualización, las estaciones de trabajo conectadas a la red interna y cualquier dispositivo vinculado al sistema de ventas en línea. Al aislar estos equipos, se limitará el alcance del ransomware y se protegerán otros activos críticos.

Mitigación Inmediata

Para frenar el ataque y evitar que comprometa más partes de la red, se deben tomar acciones inmediatas:

- **Cortar el acceso externo:** Desactivar de inmediato todas las conexiones externas para impedir que el atacante mantenga acceso remoto.
- **Desactivar conexiones VPN:** Suspender temporalmente las conexiones VPN para reducir la exposición de la red y evitar que el ransomware se propague.
- **Tomar snapshots:** Crear snapshots o copias de los sistemas críticos, lo que permitirá conservar una imagen exacta de los mismos para su análisis forense y facilitará la posterior recuperación.

Resiliencia Técnica

Para fortalecer la resiliencia ante posibles futuros incidentes, se recomienda implementar una

segmentación en la red que incluya entornos "air-gapped" o aislados, sin conexión directa al resto de los sistemas de EcoShop. Además, aplicar controles de acceso más estrictos, limitará los permisos de los usuarios únicamente a lo necesario, reduciendo el riesgo de propagación en caso de un nuevo ataque.

3. Comunicado de Notificación de Incidente de Seguridad a la Autoridad de Protección de Datos

Estimados miembros de la Autoridad de Protección de Datos,

Mediante esta notificación, informamos sobre un incidente de seguridad ocurrido en EcoShop, una tienda en línea dedicada al comercio electrónico. El día 2 de noviembre de 2024, detectamos actividad sospechosa que reveló un ataque de ransomware, probablemente causado por un correo de phishing. Este incidente ha afectado la disponibilidad de nuestros servicios y ha comprometido ciertos datos personales de nuestros clientes.

Descripción del Incidente

El ataque permitió un acceso no autorizado a nuestra infraestructura, causando interrupciones en las operaciones y exponiendo información de clientes. Los datos posiblemente comprometidos incluyen nombres, direcciones de correo electrónico y detalles de pedidos. Estamos trabajando para precisar el alcance completo de los datos afectados.

Medidas Implementadas

Desde que detectamos el ataque, tomamos medidas inmediatas para contener la situación, incluyendo el aislamiento de los sistemas afectados y la suspensión de conexiones externas. Además, estamos llevando a cabo un análisis forense para entender cómo se llevó a cabo el ataque y garantizar que no queden vulnerabilidades en nuestros sistemas. También hemos reforzado nuestras defensas en colaboración con especialistas en ciberseguridad para prevenir futuros incidentes.

Plan de Comunicación para Clientes Afectados

Estamos preparando un comunicado para informar a los clientes cuyos datos pudieron verse comprometidos. En este aviso, explicaremos el tipo de datos que pudieron ser expuestos y daremos recomendaciones para proteger su información personal. También incluiremos pautas para que los clientes refuercen la seguridad de sus cuentas y estén atentos a posibles intentos de fraude.

Agradecemos su atención y quedamos disponibles para cualquier consulta adicional que pueda surgir en el proceso de resolución de este incidente, en cumplimiento con las normativas del GDPR.

Atentamente,

Equipo de Seguridad y Cumplimiento de EcoShop

Paso 2: Recuperación y Resiliencia

Restauración de Sistemas Críticos

Para asegurar la recuperación efectiva de los sistemas críticos de EcoShop, hemos diseñado un Plan de Recuperación siguiendo los lineamientos del BCRA y el NIST CSF 2.0. Este plan incluye los siguientes pasos clave:

Restauración desde Copias de Seguridad

Antes de restaurar los sistemas críticos, verificaremos la integridad de las copias de seguridad. Para ello, realizaremos una revisión detallada en un entorno de prueba aislado, donde se someterán las copias a análisis de seguridad y pruebas funcionales para confirmar que están libres de malware o ransomware. Solo después de asegurar que las copias son seguras, procederemos a restaurarlas en el entorno de producción.

Infraestructura VMware

El ataque aprovechó una vulnerabilidad en nuestra infraestructura de VMware, por lo que tomaremos varias medidas para corregir y reforzar la seguridad de estos sistemas:

1. **Aplicación de parches de seguridad:** Instalaremos todas las actualizaciones recomendadas por VMware para cerrar la brecha de seguridad utilizada en el ataque.
2. **Revisión de posibles puertas traseras:** Realizaremos una revisión exhaustiva de los sistemas en busca de software o accesos no autorizados. Esto incluirá el análisis de puertos abiertos y la revisión de los registros de actividad para detectar cualquier signo de acceso sospechoso.

Control de Acceso y Monitoreo

Para proteger los sistemas restaurados, implementaremos políticas de segmentación de red y control de acceso basado en roles. Esto limitará el acceso a los sistemas críticos únicamente a los usuarios que lo necesiten para sus funciones específicas. Además, activaremos un monitoreo continuo para detectar de inmediato cualquier intento de acceso no autorizado y responder rápidamente ante posibles amenazas. Este enfoque nos permitirá restaurar los sistemas críticos de EcoShop de manera segura y controlada,

fortaleciendo la infraestructura y reduciendo el riesgo de futuros incidentes.



Informe de Mejora Continua

Con base en la fase de mejora continua del NIST CSF, se identificaron algunas áreas que necesitan reforzarse para que EcoShop esté mejor preparado frente a futuros ciberataques. Este informe abarca la evaluación de riesgos, la capacitación interna y la incorporación de herramientas avanzadas de detección y respuesta.

Evaluación de Riesgos

El análisis del incidente reveló ciertos factores que facilitaron el ataque:

- **Deficiencias en la segmentación de la red:** La falta de segmentación adecuada permitió que el ransomware se propagara a otros sistemas.
- **Vulnerabilidades sin parches:** Se detectó una vulnerabilidad en la infraestructura de VMware que no había sido corregida, lo cual fue aprovechado para ejecutar el ransomware.
- **Errores humanos:** El ataque fue iniciado mediante un correo de phishing que fue abierto sin precaución, lo que demuestra la necesidad de mejorar la concientización en ciberseguridad.

Para abordar estos puntos, recomendamos una segmentación de red más estricta, una gestión de parches más proactiva y controles adicionales para reducir el riesgo de errores humanos.

Capacitación Interna

Proponemos implementar un programa de capacitación continua en ciberseguridad para todos los empleados de EcoShop, con especial énfasis en la detección de correos de phishing y otras tácticas de ataque comunes. Además, se llevarán a cabo simulacros periódicos de phishing para evaluar la habilidad del equipo en reconocer y evitar estos intentos de ataque. Esto ayudará a crear una cultura de ciberseguridad más sólida y reducirá la probabilidad de incidentes causados por errores humanos.

Implementación de Nuevas Herramientas de Detección

Para fortalecer la capacidad de respuesta ante amenazas, recomendamos adoptar herramientas avanzadas de ciberseguridad, como soluciones SOAR (Security Orchestration, Automation, and Response). Estas herramientas permitirán automatizar ciertas respuestas ante incidentes, reducir el tiempo de reacción y optimizar las operaciones de seguridad. La automatización de procesos repetitivos también permitirá que el equipo de seguridad pueda concentrarse en amenazas más complejas y en la gestión de riesgos de mayor impacto.

Paso 3: Gestión del Incidente con Terceras Partes

Evaluación y Gestión de Proveedores

El ataque cibernético puso en evidencia algunas vulnerabilidades en los servicios proporcionados por terceros. Para asegurarnos de que estos proveedores cumplan con los estándares de seguridad de EcoShop, y en línea con los requisitos de la comunicación "A" 7777 del BCRA, se ha elaborado un formulario de seguridad que deberán completar y cumplir.

- **Compromiso con Pruebas de Seguridad:** Se requiere que los proveedores realicen pruebas de penetración periódicas en sus sistemas, identificando y corrigiendo posibles vulnerabilidades. Además, deberán entregar a EcoShop informes de auditoría de seguridad, detallando los resultados de estas pruebas y las medidas implementadas.
- **Protección de Datos:** El formulario incluirá cláusulas que especifiquen las responsabilidades de los proveedores en cuanto a la protección de los datos, junto con las consecuencias por incumplimiento. Esto implica que, si los datos de EcoShop o de sus clientes se ven comprometidos debido a fallos de seguridad en sus servicios, el proveedor será responsable de los daños ocasionados.

Auditoría de Seguridad

Para asegurar que los proveedores cumplan continuamente con los requisitos de seguridad, se ha desarrollado un Plan de Auditoría basado en los lineamientos de la ISO 27001. Este plan permitirá hacer revisiones periódicas para evaluar la efectividad de los controles implementados por los proveedores.

- **Metodología de Auditoría:** La auditoría se llevará a cabo bajo criterios específicos, como la eficacia de los controles de acceso, el uso de encriptación en datos sensibles y el grado de cumplimiento con las políticas de seguridad acordadas. También se revisarán los informes de las pruebas de seguridad y las acciones correctivas realizadas por el proveedor.
- **Revisión de Contratos:** Se revisarán los contratos con los proveedores para asegurar que incluyan derechos de auditoría y sanciones en caso de incumplimiento de los estándares de seguridad. Esto permitirá a EcoShop realizar auditorías periódicas y, en caso necesario, aplicar medidas correctivas para proteger su infraestructura y datos.

Paso 4: Ejercicio de Resiliencia del NIST 2.0

Universidad del Gran Rosario

Simulación de Ciberataque y Evaluación

Para mejorar la capacidad de EcoShop en la respuesta a incidentes de ciberseguridad, se propone un simulacro de ciberataque que imite el reciente ataque de ransomware. Este ejercicio se dividirá en las siguientes fases:

- Fase de Detección**
En esta etapa, el equipo aprenderá a identificar señales tempranas de un posible ransomware. Las señales de alerta incluyen actividad inusual en los registros de acceso y patrones anómalos en el tráfico de la infraestructura de VMware. Las herramientas principales serán el EDR (Endpoint Detection and Response) para monitorear dispositivos finales, y un sistema SIEM (Security Information and Event Management) que permitirá analizar eventos de seguridad y rastrear accesos no autorizados.
- Fase de Respuesta Inmediata**
Una vez detectado el ataque, se pondrá en marcha un plan de respuesta que coordine a los equipos de TI, ciberseguridad y alta dirección. Este plan incluye:
 - Aislar los sistemas afectados para evitar que el ransomware se propague.
 - Desconectar conexiones externas, incluidas las VPN, para reducir la posibilidad de acceso remoto no autorizado.
 - Asegurar una comunicación clara y rápida entre los equipos para coordinar la respuesta.
 - Activar el protocolo de notificación a clientes si se confirma que su información personal podría haberse visto comprometida.
- Fase de Recuperación**
Durante la fase de recuperación, se evaluará si el tiempo de restauración de los sistemas críticos cumple con los objetivos del NIST CSF 2.0. Además, se realizarán análisis de seguridad para confirmar que los sistemas restaurados están libres de vulnerabilidades residuales. Este proceso incluye escaneos detallados y revisiones en busca de puertas traseras o software malicioso que pudiera haber quedado.

Métricas de Evaluación

Para evaluar el éxito del simulacro y la preparación de EcoShop, se usarán métricas basadas en las funciones de **Responder** y **Recuperar** del NIST CSF 2.0:

Métrica	Descripción
Tiempo de Respuesta	Tiempo desde la detección inicial hasta la contención del ataque.
Eficacia de la Recuperación	Porcentaje de sistemas críticos restaurados en las primeras 48 horas del incidente.
Impacto en la Reputación	Proyección de impacto en clientes y proveedores según la comunicación del incidente.

Paso 5: Redacción de Formularios y Políticas de Cumplimiento

Formulario de Consentimiento de Clientes (GDPR)


Propósito: EcoShop, en cumplimiento con el Reglamento General de Protección de Datos (GDPR), solicita su consentimiento para recopilar y utilizar sus datos personales.

Elemento	Descripción
Recopilación y Tratamiento de Datos	Uso para comunicaciones de marketing y análisis de comportamiento de compra.
Retiro del Consentimiento	Opción para contactar atención al cliente o modificar preferencias en la cuenta.

Política Interna de Gestión de Ciberincidentes

Propósito: Esta política tiene como objetivo proporcionar un marco para la detección, notificación y respuesta a ciberincidentes en EcoShop, alineado con ISO 27001 y los lineamientos del BCRA.

Proceso	Acción
---------	--------

Detección y Notificación		Monitorear sistemas continuamente; notificar autoridades en 72 horas si hay incidentes.
Coordinación con Proveedores		Comunicarse con proveedores en caso de incidente y coordinar respuesta.

Acuerdo de Nivel de Servicio (SLA) para Proveedores

Propósito: Este acuerdo establece los compromisos de seguridad que los proveedores deben cumplir al ofrecer servicios a EcoShop, en conformidad con ISO 27001 y el BCRA.

Elemento	Descripción
Garantías de Seguridad	Los proveedores deben comprometerse a mantener auditorías de seguridad y protección de datos.
Derechos de Auditoría	EcoShop puede realizar auditorías para asegurar cumplimiento; sanciones en caso de incumplimiento.

3. ANEXO

Nota: Las mejoras detalladas de los formularios preventivos para clientes, proveedores y empleados se encuentran disponibles en los siguientes enlaces web. Estos enlaces se incluye versiones ampliadas y profesionalizadas de los formularios, alineadas con los marcos normativos BCRA, ISO 27001, NIST CSF 2.0 y GDPR.

- <https://form.jotform.com/243110879919061> (clientes)
- <https://form.jotform.com/243111809846054> (proveedor)
- <https://form.jotform.com/243111578019049> (empleados)

4. CONCLUSIONES

A lo largo de la lectura de las actividades y el desarrollo del trabajo, pude comprender el gran valor práctico que este ejercicio aporta. La actividad y el trabajo ya desarrollado sirven como una documentación útil para la vida laboral real, actuando como una guía estructurada que podría aplicarse en situaciones similares, aunque adaptándose a las variables específicas de cada caso. Además, quisiera resaltar la eficacia del método práctico para integrar y combinar distintos marcos normativos como una estrategia integral de ciberseguridad. Este enfoque facilita la comprensión y aplicación de cada norma en conjunto, ofreciendo una visión holística que es esencial en la protección de la información y la resiliencia organizacional.

5. REFERENCIAS

Banco Central de la República Argentina. (s.f.). *Ciberseguridad.*
<https://www.bcra.gob.ar/SistemasFinancierosYdePagos/Ciberseguridad.asp>

Universidad de Granada. (s.f.). *Caso práctico 27001.*
[https://virtual.ugr.edu.ar/pluginfile.php/468266/mod_resource/content/1/caso%20practico%2027001%20spl](https://virtual.ugr.edu.ar/pluginfile.php/468266/mod_resource/content/1/caso%20practico%2027001%20splash.pdf)
[ash.pdf](https://virtual.ugr.edu.ar/pluginfile.php/468266/mod_resource/content/1/caso%20practico%2027001%20splash.pdf)

Universidad de Granada. (s.f.). *NIST vs ISO 27001: Marcos de Ciberseguridad.*
https://virtual.ugr.edu.ar/pluginfile.php/495705/mod_resource/content/4/NIST-vs-ISO-27001-Marcos-de-Ciberseguridad.pdf

National Institute of Standards and Technology. (2020). *Cybersecurity Framework: A Spanish Translation.* <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf>

Unión Europea. (2016). *Reglamento General de Protección de Datos (GDPR).*
[https://virtual.ugr.edu.ar/pluginfile.php/333372/mod_resource/content/1/UE%20GDPR%20Texto%20Origin](https://virtual.ugr.edu.ar/pluginfile.php/333372/mod_resource/content/1/UE%20GDPR%20Texto%20Original.pdf)
[al.pdf](https://virtual.ugr.edu.ar/pluginfile.php/333372/mod_resource/content/1/UE%20GDPR%20Texto%20Original.pdf)

Jotform. (s.f.). Mis formularios. <https://www.jotform.com/es/myforms/>

Este documento sigue las normas de citación y referencias de la *Publication Manual of the American Psychological Association* (7ª ed.).