INDUSTRIA DE LICORES DEL VALLE

890.399.012-0

N° SC 639-1

GESTION TECNOLOGICA

PLAN DE RECUPERACION DE DESASTRES Y MITIGACION DE RIESGOS EN CASO DE ATAQUE CIBERNETICO

HEBERT ARTURO SEGURA MOLLANO
Jefe de Sistemas

Fecha: Diciembre 15 de 2025

INTRODUCCION

Los ataques aumentan su frecuencia cada año, afectando a multitud de empresas y particulares. Hasta hace poco tiempo, muchas empresas creían que los ciberataques eran algo ajeno para ellas, pues ¿Quién querría atacar un pequeño negocio habiendo tantas compañías grandes? Sin embargo, cualquier empresa, independientemente de su tamaño y sector, debe estar preparada para enfrentar los incidentes de seguridad.

Tras estas recomendaciones, es el momento de dar los primeros pasos:

1. Evaluar el incidente. Cuando sospechas si estás recibiendo un ataque informático en tus sistemas, es importante identificar la gravedad del suceso, registrar los datos recogidos y revisar los sistemas de la empresa.

2. Comunicar el incidente. Al principio, se recomienda que solo las personas que puedan servir de ayuda a lo ocurrido sepan del ataque, ya que corre riesgo la reputación de la empresa.

3. Contener los daños. Para ello, es importante actuar con rapidez y eficacia. Teniendo en cuenta que el tiempo es un factor diferencial, tardar demasiado en actuar podría desencadenar un problema mucho más grave. Por eso, recuerda priorizar la seguridad de las personas, la información más valiosa de la empresa y los equipos o sistemas.

Los ataques informáticos son uno de los mayores problemas de las empresas en España, y los más comunes son: el ransomware (malware que entra en el ordenador para cifrar los datos y pedir un rescate económico a cambio de liberar el ataque), el adware (afecta a usuarios individuales) y el phishing (suplantación de identidad con el fin de obtener los datos de tarjetas de crédito cuentas bancarias), entre otros.

OBJETIVOS GENERALES

Un ciberataque es un intento malicioso de acceder, dañar o robar datos de sistemas y redes. El secuestro de información o *Ransomware* es un tipo específico donde malware cifra archivos, bloqueando el acceso a ellos para exigir un rescate económico, a menudo filtrando datos sensibles si no se paga

1. Mantener la calma: No actúe por impulso ni apague los equipos inmediatamente (puede perder evidencia en la memoria RAM), desconéctelos de la red (WiFi o cable) para frenar la propagación.

2. Aislar los sistemas: Desconecte los equipos infectados de internet y de la red interna. Si es un servidor, aíslelo a nivel de red.

3. Evaluar el alcance: Identifique qué sistemas, datos (personales, bancarios) y cuentas han sido afectados.

4. Documentar todo: Registre los hechos: fecha, hora, tipo de ataque, comportamientos extraños y acciones tomadas.

5. Cambiar credenciales: Cambie todas las contraseñas de las cuentas comprometidas y de sistemas críticos desde un dispositivo limpio

OBJETIVOS ESPECIFICOS

Los ciberdelincuentes se encuentran al acecho, de nuevas maneras con las que atacar a los usuarios., tales como:

Aspectos clave de ciberataques y secuestro (Ransomware)

-Proceso de ataque: Generalmente incluye distribución (ej. correos phishing), infección, cifrado de datos, notificación de rescate y extorsión.

-Impacto: Provoca interrupción operativa, pérdidas financieras millonarias, daño reputacional y pérdida permanente de datos

- **Ataques a contraseñas**

Utilizar la misma contraseña para acceder a distintas aplicaciones, apuntarlas en notas, guardarlas en el navegador o usar contraseñas demasiado fáciles de recordar puede acarrear graves consecuencias. Algunos de los ataques más comunes son: fuerza bruta y ataque por diccionario.

- **Ataques de ingeniería social**

Están basados en el uso de técnicas orientadas a los usuarios para obtener información personal. Son ataques informáticos basados en el engaño y en la manipulación. Por ejemplo: phishing.

- **Ataques a las conexiones**

Son de los ciberataques más comunes en las empresas y están basados en la interrupción del intercambio de datos entre el usuario y el servicio web. Algunos de los ataques a las conexiones más comunes son: redes trampa y spoofing.

PROTECCION DE DATOS

SISTEMAS DE GESTIÓN DE ACCESOS.

Un sistema de gestión de accesos, contraseñas e identidades es una herramienta que ayuda a administrar y controlar el acceso de los usuarios a los sistemas de una organización.

Estos sistemas permiten a las empresas monitorizar y gestionar las credenciales de acceso de los usuarios, administrar el acceso a los recursos, así como administrar y almacenar contraseñas con seguridad.

Esto ayuda a asegurar que los usuarios no tengan acceso a recursos no autorizados y a proporcionar una mayor seguridad para los datos y recursos corporativos. En 2025, la gestión de accesos, contraseñas e identidades será aún más importante para la ciberseguridad debido a que los atacantes están constantemente buscando nuevas formas de acceder a los datos confidenciales.

SISTEMAS DE GESTIÓN DE COPIAS DE SEGURIDAD

Esta solución se centra en gestionar el proceso de copia de seguridad, incluyendo el almacenamiento bien sea Local o en la Nube, y el respaldo debe estar garantizado dentro del proceso de TI, el otro punto es la recuperación de datos y la administración de la seguridad.

Este servicio asegura que los datos estén protegidos frente a virus informáticos, ataques de Ransomware y otros problemas de seguridad. Además, ofrece herramientas para la recuperación de datos en caso de una pérdida, lo que significa que una empresa puede recuperar rápidamente sus datos sin perder tiempo ni dinero

RECUPERACION DE DATOS ANTE DESASTRES DE ATAQUES CIBERNETICOS

La recuperación ante desastres es una estrategia de ciberseguridad cuyo objetivo es garantizar que una empresa pueda seguir funcionando sin interrupción en caso de un fallo catastrófico. Esto se hace a través de backups regulares y planes de recuperación y contingencia que se pueden utilizar para restaurar los sistemas y el negocio en caso de un desastre o una crisis de seguridad.

Esta estrategia se vuelve cada vez más importante a medida que la tecnología avanza y la presión de la ciberseguridad aumenta. En 2023, la recuperación ante desastres será una parte crítica de la estrategia de ciberseguridad de cualquier empresa, ya que la recuperación de datos debe ser rápida.

Al margen de estas medidas, también es importante asegurarse de que los dispositivos están actualizados con la última versión de software y que la seguridad está configurada para protegerlos contra accesos no autorizados. Al disponer de un Centro de Operaciones de Seguridad de la Información, no tendrás que preocuparte por las actividades de detección y seguridad analítica, ellos lo harán por ti.

En resumen, es importante estar preparado para proteger los datos de tu organización a lo largo de este año. Esto significa que debes tomar medidas para mejorar la seguridad en la nube, establecer una política de seguridad, estar al día en los últimos servicios de seguridad y proteger debidamente los dispositivos de tu empresa.

Estas medidas te ayudarán a garantizar que los datos corporativos estén seguros y protegidos contra las principales amenazas de ciberseguridad.

Descripción del ataque Cibernético presentado en la Industria de Licores del Valle.

Que el pasado 28 de octubre de 2024, los sistemas de la ILV, específicamente el servidor de dominio y de la red, fueron atacados por un RANSOMWARE, que bloqueo y encripto la información que contenía los servidores, el mencionado ataque se realizó por medio de una VPN denominada Guest o invitado, e ingresaron por el equipo de seguridad perimetral denominado Fortinet 200E, encriptando toda la información de la Red, el dominio, y varios servidores virtuales que se tenían en ese servidor impactado, por tal motivo se debe volver todo a su normalidad restableciendo el servicio de Red y dominio y los demás servicios que existían en las máquinas virtuales.

De acuerdo con lo anterior y con el propósito de restablecer los servicios a los usuarios de la ILV, se contrataron varias Empresa especialista en temas de Ciberseguridad para que realizara una investigación exhaustiva y suministrara un informe técnico de lo sucedido., al igual que configurara nuevamente el Servidor impactado y estableciera protocolos de máxima seguridad que brindarán una mayor protección a la plataforma tecnológica.

Problema presentado en el ataque del Ransomware:

Según un estudio presentado por la empresa **Liberty Networks**, la falla de seguridad radicó en la vulnerabilidad de una VPN (**usuario Guest**), que fue utilizada por delincuentes informáticos para ingresar al servidor virtual. Este servidor contenía las máquinas virtuales que posteriormente fueron encriptadas mediante un **RANSOMWARE** el día 28 de octubre de 2024, aproximadamente a las 22:30 horas.

Nivel de Pérdida de Información:

La última copia de seguridad disponible antes del cifrado por ransomware data del 9 de octubre de 2024. Como resultado del ataque, se perdieron 15 días de archivos comprendidos hasta el 28 de octubre de 2024, incluyendo formatos como *.pdf, *.doc, *.xls y *.jpg, pdf.

Servidores Afectados:

- ISOLUCION
- DOMINIO (RED)
- CORREO
- BACKUP
- MAGIINFO (PANTALLA INTERACTIVA -PRODUCCION)

Según un estudio presentado por la empresa especialistas en Ciberseguridad, llamada **Cuatro i,** y de acuerdo al análisis forense y criptográfico de las muestras examinadas, se detectaron patrones de cifrado altamente complejos.

El Ransomware **QILIM** opera como un Raas (Ransomware as service), según nuestro análisis este tipo de Ransomware es desarrollado por grupos independientes que utilizan diversos kits de malware disponibles en el mercado, los cuales modifican para crear sus propias variantes personalizadas, este tipo de Ransomware suele atacar principalmente equipos NAS, Maquinas virtuales y archivos de bases de datos, aunque en ciertos casos su alcance puede ser más amplio.

El Malware que se instaló en el Servidor después de sufrir el ataque por RDP, (Remote Destok Protocolo) posiblemente originado desde Rusia, presento algún tipo de conflicto con el Antivirus, sus sistemas de seguridad, e incluso y debido a la naturaleza de la variante de Qilin, limito los atributos y características de cifrado que se estaban ejecutando al momento del ataque.

Lamentablemente una de las características de Qilin es que el Malware pierde el control de sus ejecuciones y puede realizar varios cifrados continuos, dañando su objetivo primordial de dejar inservible y operativo el funcionamiento del servidor afectado.

Sensibilidad de la Información en Riesgo:
Como administrador del sistema informático de la empresa Industria de Licores del Valle, se evalúa que la información encriptada posee una sensibilidad MEDIA/BAJA debido a su relevancia operativa y administrativa.

Riesgo para la Empresa y Usuarios:
Impacto Económico: El riesgo es bajo ya que el sistema contable ARP JD Edwards no fue vulnerado., los archivos impactados en su gran mayoría Word, Exell, Power Point y PDF, reposan en el correo, el cual no sufrió por que se tenía una copia espejo en un servidor en Alemania.

Impacto en los Usuarios:
La información perdida equivale a archivos de ofimática Word – Excell- PowerPoint y PDF, generados entre la fecha del último backup seguro y el día del ataque., equivalente aproximadamente a 10 días hábiles de Información.

Acciones de Contingencia:

- Se notificó al proveedor de firewall (**Liberty Networks**) para cerrar las brechas de seguridad.
- Se alertó a los proveedores y contratistas que brindan soporte perimetral en la red de ILV.
- Se procedió al cambio de IPs públicas.
- Se recopiló información para un análisis forense a presentar ante los entes de control.
- Se activó un servidor de correo de respaldo y se compartieron archivos de backup con los usuarios para minimizar el impacto en las operaciones.

Análisis de Causas:

El ataque ocurrió el 28 de octubre de 2024 a las 22:30 aproximadamente según LOG del sistema; mediante el acceso no autorizado a través del sistema Fortinet con una VPN no autorizada.

Operatividad de Backup:
Existen copias de seguridad de los días 1, 9, 15 y 28 de octubre. Sin embargo, solo las copias de los días 1 y 9 fueron extraídas a un disco externo, mientras que las de los días 15 y 28 se vieron comprometidas por el ataque.

Tratamiento del Riesgo:

- Se cambiaron las IPs públicas, dificultando el acceso de los atacantes a través de la misma dirección web.
- Se restauró el sistema utilizando software nuevo, instalado y configurado por una empresa especializada que garantiza la protección de los servidores virtuales.
- Se implementó un esquema de copias de seguridad en cintas tres veces al día para los servidores afectados.

Evaluación de la Política de Seguridad de la Información:
El objetivo de esta evaluación es analizar la efectividad de la política de seguridad tras el ataque de ransomware y proponer mejoras para fortalecer la protección de la información.

Vulnerabilidades Identificadas:

- Falta de actualizaciones regulares de software y sistemas operativos.
- Ausencia de medidas de protección avanzadas, como el cifrado de datos sensibles.
- Políticas de acceso insuficientes que permitieron el ingreso no autorizado a información crítica.

Impacto del Incidente:

El Ransomware afectó principalmente archivos compartidos en la red, sin comprometer información financiera. No obstante, la pérdida de acceso a estos datos impactó significativamente las operaciones diarias.

Medidas de Contingencia Implementadas:

- Restauración de datos desde el último backup seguro del 9 de octubre de 2024.
- Revisión y fortalecimiento de las políticas de acceso y autenticación.
- Implementación de soluciones adicionales de seguridad, como firewalls y sistemas de detección de intrusiones.
- Revisión de la Política de Seguridad de la Información

Conclusiones y Recomendaciones

El análisis evidencia que, aunque existen medidas básicas de seguridad, es imprescindible fortalecer la política de seguridad de la información. Se recomienda:

- Establecer un calendario de actualizaciones y mantenimiento de sistemas.
- Actualizar el Equipo de Seguridad Perimetral.
- Capacitar a los usuarios de sistemas, en el manejo del Equipo de Seguridad Perimetral denominado FORTINET, para poder administrar dicho equipo con personal interno de la Industria de Licores del Valle.
- Implementar tecnologías de protección avanzadas, como el cifrado de datos y la autenticación multifactor.
- Realizar copias de seguridad de la información todos los días hábiles.
- Realizar simulacros de Restauración de Información por lo menos 2 veces al año, que garantice su funcionalidad.
- Realizar auditorías periódicas de seguridad y simulacros de respuesta a incidentes.

Atentamente,

HEBERT ARTURO SEGURA MOLLANO
Jefe de Sistemas

Copia: Archivo