Instituto Tecnológico y de Estudios Superiores de Occidente

Reconocimiento de validez oficial de estudios de nivel superior según acuerdo secretarial 15018, publicado en el Diario Oficial de la Federación el 29 de noviembre de 1976.

Departamento de Electrónica, Sistemas e Informática

MAESTRÍA EN INFORMÁTICA APLICADA

IMPACTO DE ATAQUE CIBERNÉTICO, RETOS Y ESTRATEGIAS DE RESILIENCIA

Trabajo recepcional para obtener el grado de

MAESTRA EN INFORMÁTICA APLICADA

Presentan: Verónica Del Carmen Soberano Torres

Asesor: Mtro. Ricardo Salas Mejía

San Pedro Tlaquepaque, Jalisco. noviembre de 2024

Contenido

Antecedentes del proyecto reportado. 3

Objetivo del proyecto reportado. 3

Justificación 3

Capítulo 1 7

Marco Teórico. 7

Capítulo 2 25

Descripción de la metodología empleada. 25

Planeación o Cronología del proyecto. 26

Capítulo 3 27

Descripción de actividades 27

Lecciones aprendidas 41

Conclusiones: 71

Bibliografía 73

Antecedentes del proyecto reportado.

Red de Carreteras de Occidente ("RCO") opera más 873 kilómetros de carreteras y autopistas, de las cuales más de 700 km son de peaje y operan bajo la marca comercial Red Vía Corta. Nuestra red de autopistas y carreteras comunica al occidente con el Bajío y centro del País. Como mejor referencia, somos la vía corta entre Guadalajara y la Ciudad de México. Conectamos además a ciudades tan importantes como León, Morelia, Aguascalientes, Querétaro e Irapuato. Ahora también contribuimos para que nuestros usuarios lleguen a ciudades como San Blas y Zamora en menos tiempo. Además de las autopistas se cuenta en cada caseta de cobro 24/7 (tienda de servicio) cuarto de kilo y *Subway.* La organización tiene alrededor de 1200 empleados a lo largo de la autopista y cuenta con 200 servidores y 800 equipos de cómputo.

Objetivo del proyecto reportado.

Minimizar el daño, restaurar la funcionalidad completa de los sistemas afectados lo más pronto posible y lo más importante asegurar medidas para prevenir futuros ataques.

Justificación

Las compañías no estamos preparadas para que un ataque de *ransomware* afecte datos, servicios y continuidad de negocio, una vez que el ataque fue concretado es primordial minimizar el daño, al tener una respuesta efectiva y rápida la propagación del virus se minimiza protegiendo la información de la compañía, tomarse el tiempo para diseñar una estrategia a pesar del caos que en ese momento se tiene en la operación es esencial para restaurar operaciones de una manera estratégica y por ultimo pero no menos importante diseñar una estrategia de ciberseguridad robusta, esto trae una evaluación del tiempo de respuesta, del tiempo de recuperación, se implementan mejoras para prevenir futuros incidentes lo que hace que la seguridad se fortalezca en todos los sentidos.

La aparición de un ataque de *ransomware* en la red OT (casetas de cobro y negocios) de RCO marcó el inicio de una situación crítica para la organización. El *ransomware,* un tipo de software malicioso diseñado para secuestrar información actúa cifrando los archivos de los dispositivos afectados, dejándolos inaccesibles. Posteriormente, los atacantes exigen un pago a cambio de la clave de descifrado necesaria para recuperar los datos.

En este caso, el ransomware conocido como "Akira" comprometió una parte significativa de los equipos conectados a la red interna de RCO. El ataque afectó no solo datos y archivos sensibles, sino también la integridad de los sistemas y la continuidad de las operaciones diarias, poniendo en riesgo la estabilidad operativa de la organización.

El impacto fue inmediato y severo, afectando a múltiples departamentos y paralizando procesos esenciales para el funcionamiento normal de RCO. La red en RCO se divide en red administrativa, red IT y red OT (casetas de cobro y negocios). El *ransomware* deja este txt en los equipos infectados *Figura 1. TXT Ransomware*.

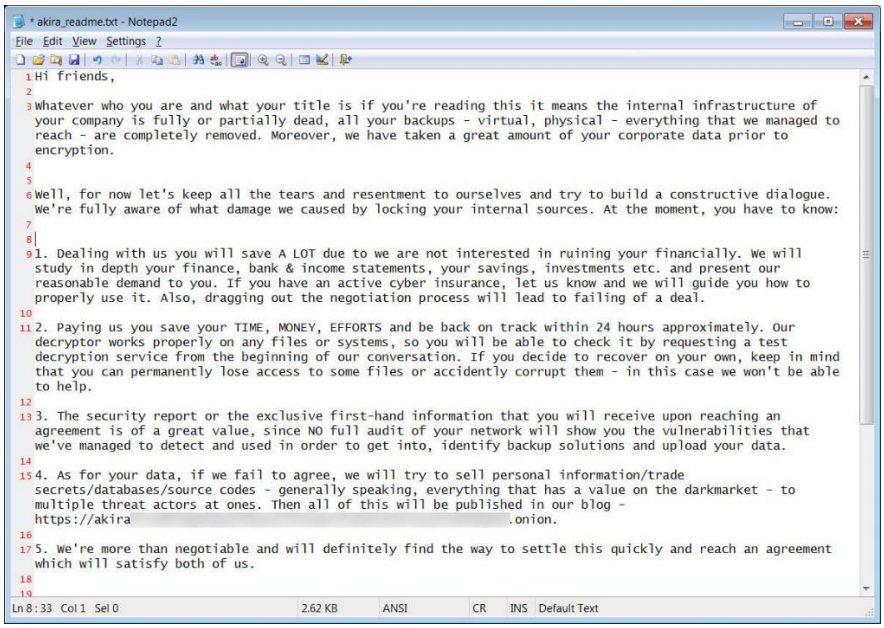


Figura 1 “TXT *Ransomware”*

El 28 y 29 de noviembre del 2023 se detectan accesos no autorizados a la red.

El 4 de diciembre del 2023 se reporta a las 8 am el despliegue del *ransomware* el cual se realizó accediendo a la VPN con una cuenta de administrador de dominio, se conectó al controlador de dominio y luego al File Server, desde donde se desplegó el *ransomware* y cifró los discos de la red de TI. No se determinó con certeza la exfiltración de credenciales de administrador y ante la ausencia de agentes EDR (*End point Detection and response*) instalados en los equipos el *ransomware* fue capaz de llegar a más equipos. Se detectó un movimiento lateral del atacante desde el segmento de red TI de RCO hacia el segmento de red de peaje FARAC donde se efectuó un segundo despliegue del *ransomware* desde el controlador de dominio de FARAC (red OT).

Durante el incidente el *ramsomware* empleo técnicas de modificación de código, des habilitación de antivirus-*firewalls* y uso de polimorfismo y metamorfismo para evitar la detección. Una vez que el *ransomware* se instala en el sistema objetivo, se encuentra en espera, recopilando datos en silencio e infectando tantos sistemas como sea posible. Luego, roba y/o encripta los archivos del sistema con los datos más valiosos y sensibles de la empresa, el atacante exige un rescate para proporcionar la clave de descifrado que permita recuperar los archivos.

Se identificaron tres áreas principales clave para la recuperación de las operaciones tras el ataque *ransomware.* En cada una de las áreas las actividades de recuperación las actividades fueron diferentes y tuvieron una prioridad distinta. A continuación, se muestran las áreas con los activos críticos identificados:

Sistemas de peaje y tráfico:

El sistema de cobro y peaje incluye nueve plazas ubicadas en diferentes lugares. Todas las plazas tienen comunicación con un servidor central que se encuentra en la joya (10 min Zapotlanejo)

- 145 carriles
- AD Farac
- Servidor central
- Servidores de vía
- Backoffice
- DVR y DVR-Replicas
- Servidor de reportes
- Equipos corporativos

Servicios corporativos: Oficinas corporativas ubicadas en Américas, la joya e Irapuato.

- Equipos corporativos – Más de 200
- Irapuato
- Nómina
- BMV (Bolsa Mexicana de Valores)
- AD Red de carreteras
- Facturación
- Timbrado
- SFTP
- Payara

Servicios auxiliares (negocios-puntos de venta, facturación)

Consisten en una serie de franquicias gestionadas por RCO Red de carreteras de occidente (algunas propias y otras con licencia de uso), fueron de las últimas actividades realizadas.

- Más de 70 equipos (POS y gerente)
- 12 servidores Linux
- 3 equipos cedis (Antigua)
- Sin afectación en servidores en AWS

Para lograr la recuperación de estas áreas críticas se precisó la coordinación de las siguientes áreas internas:

- Operaciones de TI (redes, servidores, bases de datos, mesa de ayuda) 10 personas
- Aplicaciones corporativas (SAP, nómina, facturación) 4 personas
- Seguridad de la información, 1 persona.
- Comité directivo: 7 personas
- Peaje operativo TI, 22 personas

Y la ayuda de los siguientes proveedores:

- NTTDATA: Seguridad de la información, 5 personas
- Intecfra: Servidores virtuales, 5 personas
- OneIT: NOC-SOC RCO, 9 personas
- Indra: Sistema de peaje, 12 personas
- IT 360: Sistema de centro de operaciones, 3 personas

Siendo un total de 70 personas involucradas en la recuperación de RCO.

Capítulo 1
Marco Teórico.

1. Seguridad de la información.
2. Tipos de *ransomware*
3. Técnicas de prevención ante ataques de *ransomware.*
4. Vectores de ataque de un *ransomware*
5. ¿Porque es casi imposible recuperar la información después de un ataque de ransomware?
6. Controles CIS (Center for Internet Security)
7. Plan de respuesta a incidentes
8. BIA (análisis de impacto empresarial)
9. BCP (*Business continuity plan*)
10. DRP (*Disaster recovery plan*)

1.- Seguridad de la información:

- Según la ISO/IEC 27000:2018, la seguridad de la información se podría definir como la preservación de la confidencialidad, integridad y disponibilidad de la información, así como la protección de la información contra accesos no autorizados, divulgación, alteración, destrucción y el aseguramiento de su accesibilidad cuando sea necesario.
- De acuerdo con Laudon y Laudon (2019, p.45). En su libro *"Sistemas de Información Gerenciales"*, afirman que "la seguridad de la información es un conjunto de medidas y controles que protegen los sistemas de información de una organización contra accesos, usos, divulgación, alteración y destrucción indebidos de la información y los sistemas".
- Mencionando a William Stallings, W. (2020). Seguridad de la información: Principios y práctica. Pearson. La seguridad de la información es un conjunto de medidas y controles adoptados para garantizar la confidencialidad, integridad y disponibilidad de los sistemas de información, protegiendo los activos informáticos y los datos frente a amenazas de naturaleza diversa, tales como accesos no autorizados, errores, fallos o desastres".

Según los autores coinciden en que la seguridad de la información se basa en tres principios fundamentales: confidencialidad, integridad y disponibilidad. En el ataque ocurrido en RCO, se vulneraron estos tres principios de manera significativa. En primer lugar, la confidencialidad fue comprometida, ya que el atacante logró acceder a bases de datos con información sensible de la compañía. En cuanto a la integridad, no hubo garantías de que los datos no hubieran sido alterados o sustraídos, lo que generó incertidumbre sobre la autenticidad de la información. Finalmente, la disponibilidad se vio *gravemente* afectada cuando los datos fueron cifrados, lo que nos obligó a rehacer redes, servidores y sistemas, perdiendo temporalmente el acceso a la información crítica. En RCO al momento del ataque no teníamos un sistema de gestión de la seguridad de la información, estábamos en proceso de generar las políticas y los procesos en todo al sistema, en la actualidad se crearon políticas y procesos de seguridad de la información y se creó un video para concientizar a todo el personal acerca de la importancia de salvaguardar la seguridad de la información.

2.- Tipos de ransomware:

Existen varios tipos de *malware* y *ransomware,* se categorizan según su funcionalidad, impacto y mecanismo de ataque.

- **Crypto-ransomware**
  - Descripción: Cifra los archivos del sistema y exige un rescate para restaurarlos.
  - Ejemplo**:** *CryptoLocker*.

  En el artículo de Kharraz et al. (2016**)**, titulado *"Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks*, destacan que el cifrado es el más común.

  Richardson & North (2017) en su artículo *"Ransomware: Evoution, mitigation and prevention*". Lo consideran una evolución del *ransomware* clásico, con mayor sofisticación.

- **Locker-ransomware**
  - Descripción: Bloquea el acceso al sistema, generalmente mostrando una pantalla de rescate. No cifra archivos individuales, sino que imposibilita el uso del equipo.
  - Ejemplo**:** *Police Locker.*

  Savage et al. (2015) en su artículo "*Ransomware: A Survey and Analysis of the Threat Landscape*": Destacan que este tipo suele incluir mensajes de autoridades falsas para presionar al usuario. Esta táctica se utiliza para aumentar el miedo y la urgencia de la víctima, motivando así el pago del rescate sin cuestionarlo.

- **Scareware**
  - Descripción: Muestra falsas advertencias de seguridad para convencer al usuario de pagar por una solución inexistente. Menos dañino, pero efectivo en usuarios no técnicos.
  - Ejemplo: Antivirus falsos como "*SpySheriff*".

  En el artículo de Al-rimy et al. (2018) titulado *"Ransomware Threat Success Factors, Taxonomy, and Countermeasures: A Survey and Research Directions"*, los autores destacan que el impacto psicológico que genera el *ransomware* es un factor clave para el éxito de los ataques. Este aspecto emocional y psicológico juega un papel crucial en la forma en que las víctimas reaccionan ante los ataques, afectando su toma de decisiones y aumentando las probabilidades de que paguen el rescate exigido por los atacantes.

- **Doxware (Leakware)**
  - Descripción: Amenaza con filtrar datos confidenciales a menos que se pague un rescate. Enfocado en empresas o individuos con información confidencial
  - Ejemplo: *Ransomware* asociado a datos médicos.

En el artículo de Liao et al. (2016) titulado *"Ransomware: A New Cyber Threat to Critical Infrastructures"*, los autores clasifican al *ransomware* dirigido a sectores médicos y legales como una variante emergente del *ransomware*. Esta modalidad se enfoca en atacar infraestructuras críticas y sectores específicos con alta sensibilidad de datos, aprovechando la naturaleza de la información almacenada y la urgencia de los servicios prestados en estos sectores para maximizar las probabilidades de pago del rescate.

- **Ransomware dirigido**

  - Descripción: es una modalidad de ataque en la que los ciberdelincuentes eligen deliberadamente a sus víctimas, enfocándose en organizaciones, empresas o entidades con alta capacidad de pago o con información crítica. Este tipo de ransomware se caracteriza por una planificación detallada y un enfoque personalizado que maximiza el impacto y la presión sobre la víctima.

  - Ejemplo: *Ryuk*.

Según el informe de Europol (2022) titulado *"The Internet Organized Crime Threat Assessment"*, se menciona que el *ransomware* dirigido a sectores críticos, como los sectores médicos y legales, suele involucrar ataques sofisticados perpetrados por grupos criminales organizados. En este contexto**,** Ryuk y Conti son ejemplos de dos de los grupos más notorios que han estado detrás de ataques dirigidos y extremadamente bien planificados.

- **RaaS (Ransomware as a Service)**

  - Descripción: Servicio en la *dark web* que permite a delincuentes sin conocimientos técnicos lanzar ataques. Los operadores comparten las ganancias con los desarrolladores del *ransomware*.

  - Ejemplo: REvil, unos de los grupos de Rass más conocidos, responsable de ataques masivos a empresa e infraestructuras críticas.

Según el informe de ENISA, *The European Union Agency for Cybersecurity* (2021) titulado *"Ransomware: Trends, Techniques, and Threats"*, la modalidad de *ransomware* dirigido a sectores críticos (como los sectores médicos y legales) ha democratizado el cibercrimen, haciendo que el acceso a herramientas de ataque sofisticadas sea más accesible para un mayor número de actores, incluidas entidades menos experimentadas en cibercrimen, mediante el modelo de *Ransomware-as-a-Service (RaaS*).

De acuerdo con las definiciones de los autores, estos coinciden al señalar que un *ransomware*, es un software malicioso diseñado para infiltrarse en redes, causar daño y robar información. En este contexto, *Akira*, un *ransomware*, atacó a RCO aprovechando privilegios elevados de una cuenta de administrador para vulnerar sus sistemas. Gracias a este acceso, Akira pudo sustraer información confidencial, encriptar archivos críticos, bases de datos y otros recursos esenciales, dejándolos inutilizables y afectando gravemente las operaciones de la organización. En este momento RCO no tenía un responsable de monitoreo de seguridad capacitado para actuar en caso de un comportamiento anormal de una cuenta administradora, hoy se cuenta con un SOC que monitorea cualquier comportamiento anómalo y además se cuenta con alertas con un software que detecta si un usuario administrador cambio su comportamiento.

3.- Técnicas de prevención ante ataques de Ransomware.

Podemos tener diferentes enfoques dependiendo del autor o de la organización.

- Al-rimy et al. (2018) en Zero-Day Aware Decision Fusion-Based Model for Crypto**-**Ransomware Early Detection**"**, publicado en el *International Journal of Integrated Engineering*stacan la importancia de los *backups* como la medida más efectiva.

1. **Realizar copias de seguridad periódicas**: Según Al-Rimy et al. (2018), realizar **copias de seguridad periódicas** es una de las medidas más efectivas contra el *ransomware*. Estas copias deben almacenarse en ubicaciones seguras, preferiblemente fuera de línea o en la nube, para evitar su compromiso en caso de ataque. Los respaldos regulares permiten restaurar datos y sistemas rápidamente, minimizando interrupciones y pérdidas financieras. Además, se recomienda verificar la integridad de las copias y probar periódicamente los procesos de recuperación para garantizar su funcionalidad en situaciones críticas.

2. **Actualización y parcheo del software**: Según Al-Rimy et al. (2018), mantener el software actualizado y aplicar parches regularmente es esencial para proteger los sistemas contra *ransomware*. Los atacantes suelen aprovechar vulnerabilidades conocidas en aplicaciones desactualizadas. Por ello, los autores destacan la importancia de implementar un sistema de gestión de parches que supervise y aplique actualizaciones de seguridad en tiempo real. Esto no solo reduce la superficie de ataque, sino que también refuerza la resistencia del entorno tecnológico frente a amenazas emergentes

3. **Control de acceso**: En el trabajo de Al-Rimy et al. (2018), se resalta la importancia del control de acceso como una estrategia crítica para mitigar los riesgos asociados al *ransomware*. Los autores recomiendan limitar los privilegios de los usuarios y aplicar el principio de menor privilegio, asegurando que solo los usuarios autorizados accedan a datos sensibles. Además, proponen el uso de autenticación multifactor (MFA) para fortalecer la seguridad en puntos de acceso críticos, reduciendo la probabilidad de que un atacante comprometa el sistema mediante credenciales robadas o débiles.

4. **Uso de soluciones antimalware**: Implementar software de protección contra *ransomware*, con sistemas de detección basados en comportamiento. Estas herramientas detectan y bloquean software malicioso antes de que pueda ejecutarse. Los autores recomiendan que las soluciones antimalware incluyan capacidades de detección basada en comportamiento y análisis heurístico, lo que permite identificar amenazas emergentes y variantes desconocidas. Además, enfatizan la necesidad de mantener las herramientas actualizadas para maximizar su eficacia frente a las técnicas avanzadas empleadas por los atacantes.

5. **Educación y formación de los empleados**: En el estudio de Al-Rimy et al. (2018) se destaca la educación y formación de los empleados como una de las medidas más efectivas para prevenir ataques de *ransomware*. Los autores enfatizan que los empleados deben ser capacitados regularmente en buenas prácticas de seguridad, como identificar correos electrónicos sospechosos, evitar hacer clic en enlaces desconocidos y seguir procedimientos seguros al manejar información sensible. Esta formación continua es crucial para reducir el riesgo de que los usuarios sean el punto de entrada de ataques cibernéticos.

6. **Segmentación de red:** En el trabajo de Al-Rimy et al. (2018), la segmentación de red se propone como una estrategia eficaz para limitar la propagación de *ransomware.* Al dividir la red en segmentos más pequeños y aislados, se reduce el riesgo de que un ataque afecte a todo el sistema. Esto permite controlar mejor el acceso y mitigar los daños al contener el programa maligno en una sección específica, evitando que se propague rápidamente a otras partes de la infraestructura**.**

7. **Monitorización de tráfico de red**: En el trabajo de Al-Rimy et al. (2018), la monitorización del tráfico de red se presenta como una medida clave para detectar y prevenir actividades sospechosas asociadas con el *ransomware.* Esta estrategia implica supervisar continuamente el tráfico en busca de patrones inusuales, como conexiones desconocidas, transferencias de datos anómalas o intentos de acceso no autorizados. Al implementar herramientas de análisis de red, las organizaciones pueden identificar ataques en sus primeras etapas y responder rápidamente para mitigar el impacto en su infraestructura.

8. **Implementación de autenticación multifactor (MFA):** En el estudio de Al-Rimy et al. (2018),) se describe como una medida esencial para fortalecer la seguridad frente al *ransomware* y otros ciberataques. La MFA combina múltiples métodos de verificación, como contraseñas, biometría o códigos enviados al dispositivo del usuario, lo que dificulta que los atacantes accedan al sistema incluso si obtienen credenciales. Esto añade una capa de protección crítica para datos sensibles y sistemas clave, minimizando la posibilidad de accesos no autorizados.

9. **Control de dispositivos USB y externos**: Al-Rimy et al. (2018) recomiendan implementar un estricto control de dispositivos USB y externos como parte de las estrategias de seguridad para prevenir la propagación de *ransomware*. Limitar el uso de dispositivos extraíbles no autorizados ayuda a evitar que archivos maliciosos sean introducidos en la red. También sugieren emplear soluciones de gestión de dispositivos que monitoreen, restrinjan y escaneen automáticamente el contenido de los dispositivos externos antes de permitir su acceso al sistema, reduciendo significativamente los riesgos de infección.

10. **Gestión de riesgos de seguridad de la información:** En el estudio de Al-Rimy et al. (2018), la gestión de riesgos de seguridad de la información se enfatiza como una práctica integral para mitigar las amenazas del ransomware. Esto implica identificar, evaluar y priorizar vulnerabilidades en sistemas y datos, además de implementar controles apropiados. La gestión debe incluir estrategias como monitoreo continuo, auditorías regulares, educación del personal y la adopción de tecnologías de defensa avanzadas. Este enfoque proactivo permite a las organizaciones reducir el impacto de los riesgos cibernéticos y fortalecer su resiliencia operativa.

De acuerdo con el CISA (*Cybersecurity & Infrastructure Security Agency*) las principales técnicas de prevención contra ataques de *ransomware* incluyen:

1. Copias de seguridad: ¿Hacemos copias de seguridad de toda la información crítica? ¿Las copias de seguridad se almacenan fuera de línea? ¿Hemos probado nuestra capacidad para volver a las copias de seguridad durante un incidente?
2. Análisis de riesgo: ¿Hemos realizado un análisis de riesgos de ciberseguridad de la organización?
3. Entrenamiento del personal: ¿Hemos capacitado al personal en las mejores prácticas de ciberseguridad?
4. Parcheo de vulnerabilidades: ¿Hemos implementado parches apropiados para las vulnerabilidades ya conocidas en el sistema?
5. Lista blanca de aplicaciones: ¿Permitimos que solo se ejecuten programas aprobados en nuestras redes?
6. Respuesta al incidente: ¿Tenemos un plan de respuesta a incidentes y lo hemos ejercido?
7. Continuidad de operaciones: ¿Somos capaces de mantener las operaciones sin acceso a ciertos sistemas? ¿Por cuánto tiempo? ¿Hemos probado esto?
8. Pruebas de penetración: ¿Hemos intentado piratear nuestros propios sistemas para probar la seguridad de nuestros sistemas y nuestra capacidad para defendernos de los ataques?

Podemos concluir que, al momento del ataque en RCO, enfrentábamos múltiples deficiencias en nuestras medidas de seguridad. El software crítico no estaba actualizado, lo que impedía la aplicación de parches necesarios para corregir vulnerabilidades. Aunque se contaba con controles de acceso, estos no eran monitoreados de manera efectiva. Los sistemas antimalware aún estaban en proceso de instalación, y aunque la red era monitoreada, carecía de los controles esenciales para detectar y mitigar amenazas. Las acciones para abordar las vulnerabilidades estaban en marcha, pero el ritmo era insuficiente para garantizar una protección adecuada frente a un ataque de esta magnitud.

Las demás medidas de seguridad sí se encontraban implementadas. Actualmente, en RCO se han implementado todas estas medidas, pero aún faltan los planes de contingencia y las políticas formalizadas. No contar con un plan de respaldo en una ubicación distinta a la principal representa un riesgo considerable, no solo en caso de un ataque de *ransomware*, sino también ante posibles daños físicos a la infraestructura. Además, la falta de procesos y políticas documentadas puede generar un riesgo elevado debido a la rotación de personal, ya que la falta de documentación puede dificultar la continuidad de las operaciones y la gestión adecuada de la seguridad.

4. **Vectores de ataque de *ransomware*:**

Los vectores de ataque son las vías o métodos que los atacantes cibernéticos utilizan para comprometer sistemas, redes o dispositivos. A continuación, se detalla una clasificación basada en múltiples autores y organismos de seguridad.

1. Phishing y Spear Phishing

Se trata de ataques que utilizan correos electrónicos maliciosos para engañar a los usuarios y obtener credenciales o instalar malware.

De acuerdo con Verizon (2024) Data *Breach Investigations Report* (DBIR): El phishing es el vector más común en violaciones de datos. A menudo contiene enlaces o archivos adjuntos que, al abrirse, ejecutan código malicioso.

En el artículo de Kharraz et al. (2016) titulado *"SpearPhishing: A comprehensive study on targeted phishing attacks"* describe cómo el *spear phishing* es una variante más sofisticada y dirigida del *phishing* tradicional, en la cual los atacantes personalizan los mensajes de correo electrónico para que parezcan provenir de fuentes confiable.

2. Explotación de Vulnerabilidades

Aprovechamiento de fallas conocidas en software o hardware

Richardson & North (2017), *ransomware*: Evolution, *Mitigation and Prevention*. Las vulnerabilidades en sistemas no actualizados son uno de los principales vectores de *ransomware*.

En su informe de 2022, Europol resalta la explotación de vulnerabilidades no parchadas como una de las principales tácticas utilizadas por ciberdelincuentes en ataques de *ransomware*. Se enfatiza que los *exploits* como *EternalBlue*, utilizado en el ataque de *WannaCry,* demuestran cómo las vulnerabilidades conocidas en sistemas y aplicaciones no actualizados pueden ser aprovechadas para causar daños masivos. A pesar de que se han lanzado parches y actualizaciones para mitigar estos riesgos, muchas organizaciones siguen siendo vulnerables debido a la falta de aplicación de estas medidas de seguridad**.**

3. Ingeniería Social

Manipulación psicológica para obtener acceso a información o sistemas.

Mitnick & Simon (2011**)**, en su obra *The Art of Deception: Controlling the Human Element of Security*, explican que la ingeniería social es uno de los métodos más efectivos y menos costosos utilizados por los atacantes. Según Mitnick, esta técnica es más eficiente que el hacking tradicional, ya que, en lugar de atacar directamente a un sistema, los atacantes manipulan a las personas para obtener acceso a información sensible o sistemas sin necesidad de realizar esfuerzos técnicos complejos. Este enfoque se basa en la persuasión y la manipulación psicológica.

El estudio de Savage, K., Coogan, P., & Lau, H. (2015). "*Ransomware deployment methods and analysis. Proceedings of the 2015 IEEE International Conference on Communications "* analiza los métodos de distribución de *ransomware*, destacando que el *phishing* sigue siendo uno de los vectores más comunes para activar el malware. En este estudio se

exploran diversas técnicas de ataque, incluyendo la combinación de phishing con kits de explotación y troyanos. La investigación también aborda cómo las tácticas de ingeniería social y la personalización de mensajes en *ransomware* son utilizadas para aumentar la efectividad del ataque.

4. **Archivos Adjuntos o Enlaces Maliciosos**

Archivos o enlaces que contienen *malware.*

ENISA Agencia de la Unión Europea para la Ciberseguridad (2023): Identifica a los archivos adjuntos en correos y enlaces como vectores principales de distribución de malware.

CISA *Certified Information Systems Auditor* (2024): Recomienda verificar siempre el origen de los archivos adjuntos para evitar infecciones.

5. **Acceso a Redes Privadas y Servicios Expuestos**

Los atacantes explotan redes mal configuradas o servicios accesibles desde internet.

Shodan y Badger (2020) *French Cities Exposed: A Shodan-Based Security Study on Exposed Cyber Assets in France*. Los servicios expuestos como bases de datos o RDP son objetivos frecuentes.

CISA Certified Information Systems Auditor (2024): Recomienda deshabilitar servicios innecesarios y proteger las redes internas.

6. **Ataques Basados en Software Malicioso (Malware)**

Uso de programas diseñados para infiltrarse en sistemas.

En el studio de Al-rimy et al. (2018) en Zero-Day *Aware Decision Fusion-Based Model for Crypto-Ransomware Early Detection***"**, Los troyanos, spyware y *ransomware* se utilizan como vectores para múltiples propósitos, desde robo de datos hasta extorsión.

El estudio de Kharraz et al. (2016) titulado "*Protection and Detection of Ransomware Attacks*" aborda cómo los ataques de *ransomware* se propagan y las técnicas que emplean. En este trabajo, los autores identifican la propagación de malware mediante gusanos y *botnets* como vectores comunes, específicamente en el contexto de las redes. Explican que, al igual que los gusanos, el *ransomware* puede autorreplicarse y propagarse a través de redes conectadas, afectando múltiples dispositivos de manera autónoma, tal como ocurrió con el *ransomware TeslaCrypt*.

7. **Ataques Basados en Contraseñas**

Ataques como fuerza bruta, reutilización de contraseñas y *credential stuffing*.

De acuerdo con Verizon (2022) Data Breach Investigations Report (DBIR): Los ataques de fuerza bruta representan una alta proporción de compromisos.

El estudio de Kharraz et al. (2016) titulado "*Protection and Detection of Ransomware Attacks*" Los atacantes explotan contraseñas débiles o reutilizadas para obtener acceso.

8. Dispositivos Físicos Comprometidos

Uso de dispositivos como USB infectados para propagar malware.

Mitnick & Simon (2011), en su libro *"The Art of Deception"*, destacan cómo la ingeniería social, particularmente la técnica de insertar dispositivos físicos como USBs infectados, puede ser una forma extremadamente eficaz para los atacantes. Resaltan la facilidad con la que dispositivos aparentemente inofensivos pueden propagarse dentro de sistemas informáticos al ser insertados, sin que el usuario tenga conocimiento de la amenaza. Esta técnica aprovecha la curiosidad humana o la confianza en dispositivos externos, lo que facilita la infección de sistemas sin necesidad de interacción directa o conocimiento del malware.

CISA (2024): Recomienda políticas estrictas para el uso de medios extraíbles.

9. Redes Wi-Fi Inseguras

Los atacantes interceptan tráfico en redes no seguras.

El estudio de Savage et al. (2015) titulado *"Ransomware Deployment Methods and Analysis" Subrayan la importancia de usar VPN* en redes públicas*.*

Para concluir, los autores coinciden en que los atacantes emplean diversas rutas para infiltrarse en los sistemas con el objetivo de obtener credenciales de administración, utilizando una variedad de estrategias. Estas van desde técnicas tradicionales, como el *phishing*, hasta enfoques más sofisticados, como el compromiso de cadenas de suministro.

En el caso del ataque a RCO, los atacantes lograron obtener las credenciales de un usuario administrador a través de la VPN. Sin embargo, también intentaron acceder a la red mediante correos electrónicos maliciosos. En ese momento, RCO no había resuelto ciertas vulnerabilidades, y aunque contábamos con VPN, no existía un monitoreo adecuado de las actividades de los usuarios administradores. Además, la organización carecía de campañas de comunicación de seguridad que pudieran haber ayudado a mitigar el riesgo de estos vectores de ataque. Actualmente RCO cuenta con campañas permanentes de concientización a los usuarios en temas de seguridad y capacitaciones, las vulnerabilidades han sido detectadas con software especializados y se les da seguimiento a su solución con cronogramas y tareas de seguimiento, la VPN fue renovada en su totalidad, las políticas de contraseñas se robustecieron a 14 caracteres, entre números y letras, se cambian cada mes, hay monitoreo de los usuarios de permisos elevados, el correo electrónico tiene doble factor, antivirus, la red también cuenta con doble factor a nivel administradores.

5. ¿Por qué es casi imposible recuperar la información?

Recuperar información cifrada por *ransomware* es extremadamente difícil debido a la naturaleza avanzada y deliberadamente intrincada de estas amenazas. A continuación, se explican las principales razones de acuerdo con diferentes autores y/o asociaciones:

1. Cifrado de grado militar

Autores como Kevin Mitnick (*The Art of Invisibility*, 2017) explican que el *ransomware* utiliza cifrados de alto nivel como AES-256 o RSA, diseñados para ser indescifrables sin la clave. Estas técnicas de cifrado están destinadas a proteger datos sensibles incluso contra ataques de supercomputadoras.

2. Claves únicas por dispositivo o archivo

Bruce Schneier en su libro Data and Goliath (2015) enfatiza que la generación de claves únicas está diseñada para evitar soluciones universales de descifrado. En variantes más sofisticadas, incluso si los expertos logran descifrar una clave para un dispositivo, no podrán usarla para descifrar otros debido a la singularidad de las claves.

3. Destrucción de herramientas de recuperación locales

El *ransomware* moderno, como explica *Bruce Schneier (Data and Goliath, 2015),* a menudo busca y destruye copias de seguridad almacenadas localmente o en la nube accesible. Además, algunas variantes deshabilitan puntos de restauración del sistema.

4. Evolución constante del *malware*

Autores como Kim Zetter (*Countdown to Zero Day*, 2014) señalan que el *ransomware* evoluciona rápidamente, creando nuevas variantes que superan las soluciones de descifrado existentes. Este avance constante asegura que los intentos de descifrado queden obsoletos rápidamente.

En resumen, durante el ataque de ransomware a RCO, varios equipos fueron cifrados, lo que resultó en la pérdida total de la información almacenada en ellos. No obstante, pudimos recuperarnos gracias a los respaldos que teníamos, los cuales estaban protegidos mediante cifrado, lo que impidió que fueran comprometidos durante el ataque. Además, dichos respaldos contaban con la última actualización de seguridad, lo que nos permitió mantenernos un paso adelante frente a la evolución constante de las amenazas. Debido a que la información no fue cifrada, los ciberdelincuentes no solicitaron rescate ni pudieron filtrar ningún dato sensible de la empresa. Actualmente, hemos reforzado la seguridad de nuestros respaldos, incrementando el nivel de cifrado, utilizando contraseñas más complejas y aplicando claves únicas para cada dispositivo.

Controles CIS. Center for Internet Security. (n.d.). *CIS Controls v8*. Center for Internet Security. Recuperado el 20 de noviembre 2024, https://www.cisecurity.org/controls/v8

Los Controles CIS (*CIS Controls*) son un conjunto de prácticas recomendadas diseñadas para ayudar a las organizaciones a protegerse contra las amenazas de ciberseguridad más comunes y críticas. Fueron desarrollados por el *Center for Internet Security* (CIS), basándose en la experiencia de expertos de todo el mundo. Los controles están organizados por prioridades, lo que permite a las organizaciones enfocar sus esfuerzos en medidas con mayor impacto en la seguridad. Actualmente, los controles CIS se encuentran organizados en 18 categorías, que cubren desde la gestión de dispositivos hasta la protección contra ataques. Estos controles son ampliamente utilizados en la industria como referencia para desarrollar políticas de ciberseguridad. A continuación, un resumen de las categorías de controles más relevantes:

Estructura de los Controles CIS

Los controles están divididos en tres categorías principales según su nivel de prioridad y complejidad:

18 controles básicos agrupados en 3 categorías de implementación

- Los controles están clasificados según su prioridad y facilidad de implementación:
    - **IG1** (Implementation Group 1): Medidas esenciales para pequeñas organizaciones o aquellas que comienzan con la seguridad básica.
    - **IG2**: Controles adicionales que requieren más recursos y son aplicables a organizaciones medianas con mayor exposición.
    - **IG3**: Controles avanzados diseñados para organizaciones grandes o con altos riesgos de seguridad.

Número	Nombre del Control	Descripción Breve
1	Inventario de Activos Empresariales	Identificar y gestionar dispositivos conectados a la red.
2	Inventario de Software Empresarial	Gestionar aplicaciones autorizadas y detectar software no deseado.
3	Gestión de Vulnerabilidades	Identificar y remediar vulnerabilidades de forma continua.
4	Gestión de Configuraciones Seguras	Aplicar configuraciones seguras en sistemas y dispositivos.
5	Gestión de Accesos	Restringir accesos a sistemas y datos únicamente a usuarios autorizados.
6	Defensa contra Malware	Implementar herramientas para prevenir, detectar y eliminar malware.
7	Registro y Monitoreo de Actividades	Rastrear actividades para detectar anomalías o incidentes.
8	Protección de Datos	Salvaguardar la información crítica en reposo y en tránsito.
9	Protección en Redes	Defender redes contra accesos no autorizados y ataques.
10	Ciberhigiene Básica	Fomentar buenas prácticas de seguridad entre los empleados.
11	Respuesta a Incidentes	Prepararse y responder eficazmente a incidentes de seguridad.
12	Recuperación de Datos	Asegurar la recuperación confiable de sistemas y datos críticos.
13	Seguridad de Correo Electrónico y Navegación Web	Prevenir riesgos provenientes de correos electrónicos y la web.
14	Controles de Acceso y Gestión de Privilegios	Minimizar privilegios y prevenir abuso de cuentas privilegiadas.
15	Seguridad en la Cadena de Suministro	Gestionar riesgos en proveedores y socios externos.
16	Seguridad en el Desarrollo de Software	Aplicar seguridad en el ciclo de vida de desarrollo (SDLC).
17	Concientización y Entrenamiento de Seguridad	Entrenar al personal en prácticas de ciberseguridad.
18	Pruebas de Seguridad y Auditorías	Validar la efectividad de controles mediante pruebas regulares.

De acuerdo con Abertis, en RCO, los controles CIS son obligatorios según las directrices establecidas por el corporativo de Abertis en Barcelona. Mi experiencia implementándolos ha sido muy gratificante, aunque el proceso de implementación requiere un esfuerzo considerable, cada control proporciona métricas claras para evaluar su cumplimiento y efectividad. Esto no solo facilita el cumplimiento de los estándares, sino que también brinda la certeza de que la seguridad se está aplicando de manera sólida y efectiva. Antes del ataque no estaban implementados los controles en RCO.

6. Plan de respuesta a incidentes

Un plan de respuesta a incidentes (PRI) es un documento estructurado que guía a una organización en la identificación, manejo y recuperación de incidentes de seguridad.

1. Enfoque NIST (SP 800-61, Rev. 2)

El NIST propone un enfoque en cuatro fases clave:

1. **Preparación**: Desarrollar capacidades para responder eficazmente (herramientas, personal y políticas).
2. **Detección y análisis**: Identificar y evaluar incidentes a través de monitoreo, alertas y registros.
3. **Contención, erradicación y recuperación**: Limitar el impacto, eliminar amenazas y restaurar operaciones.
4. **Lecciones aprendidas**: Revisar el incidente para mejorar procedimientos futuros.

2. Modelo SANS

El SANS Institute detalla seis pasos esenciales para la respuesta a incidentes:

1. **Preparación**: Capacitación y definición de roles del equipo.
2. **Identificación**: Detectar incidentes mediante análisis de logs, alertas y reportes.
3. **Contención**: Minimizar el impacto mientras se investiga el incidente.
4. **Erradicación**: Remover amenazas y reparar sistemas afectados.
5. **Recuperación**: Restaurar operaciones normales, garantizando la ausencia de vulnerabilidades persistentes.
6. **Lecciones aprendidas**: Documentar el caso para ajustar el plan de respuesta.

3. Enfoque de Eric Cole

En su libro *"Advanced Persistent Threat, 2012"*, Eric Cole sugiere un enfoque proactivo con tres pilares:

1. **Monitoreo continuo**: Detectar comportamientos anómalos en tiempo real.
2. **Gestión de incidentes en capas**: Establecer niveles de respuesta basados en el tipo y gravedad del incidente.

3. **Evaluación de impacto comercial**: Asegurar que las acciones tomadas consideren las prioridades del negocio

4. Modelo de Michael Cobb

Michael Cobb en *"Incident response plan essentials: How to prepare for a data breach"*, publicado en SearchSecurity, enfatiza que un plan efectivo de respuesta a incidentes debe ser claro, bien documentado y probado regularmente. Según sus principios, un buen plan incluye los siguientes pasos:

1. **Preparación**: Desarrollar políticas y procedimientos, capacitar al personal y realizar simulaciones para anticiparse a posibles escenarios.
2. **Identificación**: Detectar y confirmar el incidente, recopilando información relevante.
3. **Contención**: Limitar el alcance del incidente para evitar daños adicionales.
4. **Erradicación**: Eliminar la causa del incidente, como malware o acceso no autorizado.
5. **Recuperación**: Restaurar sistemas y operaciones normales, asegurándose de que no persistan vulnerabilidades.
6. **Lecciones aprendidas**: Documentar el incidente, evaluar la respuesta y actualizar el plan para futuras contingencias.

En términos generales, durante el ataque, no contábamos con un plan de respuesta a incidentes. Esto significó que no habíamos realizado pruebas previas, desconocíamos los roles que cada uno debía asumir y no teníamos claridad sobre los pasos iniciales a seguir. Como resultado, nuestra respuesta al incidente fue completamente empírica, lo que impactó significativamente en el tiempo y esfuerzo invertidos.

Adoptamos un enfoque extremadamente drástico para recuperar las redes y los servidores. Aunque logramos restaurar los sistemas en mes y medio, este proceso resultó ser innecesariamente arduo debido a la falta de preparación, ya que optamos por rehacer todo desde cero. Esto implicó un trabajo extenuante que demandó un esfuerzo minucioso, involucrando a muchas personas, una sólida organización y un control riguroso en la administración de riesgos.

Actualmente, en RCO contamos con la primera versión de un plan de respuesta a incidentes, basado principalmente en el marco NIS (Network and Information Systems). Este plan está en proceso de aprobación y se llevarán a cabo pruebas periódicas para garantizar que, en caso de futuros incidentes, todos los involucrados sepan exactamente qué se espera de ellos y cómo actuar de manera coordinada y eficiente.

8 BIA (Análisis de impacto empresarial)

Es un proceso crítico en la gestión de continuidad del negocio (BCM) que ayuda a identificar y evaluar los efectos potenciales de interrupciones en los procesos clave de una organización. El objetivo principal del BIA es priorizar los recursos y definir estrategias de recuperación que minimicen los impactos financieros, operativos, legales y de reputación.

1. El NIST ofrece un enfoque estructurado para el BIA en su guía SP 800-34 sobre continuidad del negocio. Según el NIST, el BIA se enfoca en:

- **Identificación de procesos críticos**: Determinar qué servicios y procesos son esenciales para la operación del negocio.
- **Impacto de la interrupción**: Analizar los efectos de una interrupción en cada proceso y cómo afecta a la organización.
- **Establecimiento de prioridades**: Clasificar los procesos según su criticidad, tiempo máximo tolerable de inactividad (MTPD) y el tiempo de recuperación (RTO).
- **Desarrollo de estrategias de recuperación**: Basadas en las prioridades establecidas en el BIA.

2. ISO **22301:2019 (Gestión de Continuidad del Negocio)**

La norma **ISO 22301:2019** también ofrece directrices específicas sobre cómo llevar a cabo un BIA. Según esta norma, el BIA se debe realizar en las primeras etapas de la planificación de la continuidad del negocio y debe abordar:

- **Impacto de interrupciones**: Evaluar los efectos financieros, operacionales, legales y reputacionales de los incidentes.
- **Identificación de dependencias**: Detectar los recursos y sistemas que dependen de los procesos clave.
- **Evaluación de riesgos**: Analizar la probabilidad de ocurrencia de interrupciones y su gravedad.

3. **SANS institute (Sysadmin Audit, Networking and Security Institute)**

El **SANS Institute**, reconocido por sus enfoques prácticos en ciberseguridad, también propone un enfoque de BIA para la gestión de la continuidad empresarial. SANS destaca los siguientes pasos clave en el BIA:

- **Recopilación de datos**: Utiliza entrevistas y cuestionarios a las partes interesadas para identificar las funciones críticas del negocio.
- **Evaluación de impacto**: Analiza cómo cada proceso afectado impacta a la organización.
- **Priorización y planificación**: Asigna prioridades basadas en la severidad del impacto y las necesidades de recuperación.

4. **Eric Cole**

En su libro *"Advanced Persistent Threats"*, **Eric Cole** presenta un enfoque del BIA dentro del marco de la protección ante amenazas avanzadas, sugiriendo:

- **Monitoreo continuo**: La necesidad de observar constantemente las amenazas para identificar áreas de impacto potencial.
- **Priorización de activos**: Determinar qué activos son más valiosos para el negocio y deben ser protegidos de manera prioritaria.
- **Evaluación post-incidente**: Tras un incidente, realizar un análisis de impacto para reforzar las defensas y evitar futuros daños.

En resumen, tanto los autores como las instituciones coinciden en que la identificación de los procesos críticos es fundamental para proteger lo esencial para la empresa. Durante el incidente, nos tomó tres horas realizar este análisis sobre la marcha. Si hubiéramos tenido una evaluación del impacto en el momento del ataque, habría facilitado una respuesta más ágil y efectiva. Además, la identificación de las interdependencias nos habría permitido mejorar la priorización de acciones. Una evaluación previa del impacto también habría contribuido a una priorización más informada y basada en investigaciones previas. En RCO, ya se ha realizado un análisis BIA y hemos recibido una serie de recomendaciones. Actualmente, estamos planificando su implementación lo antes posible, y aquellas que no se puedan resolver de inmediato serán incluidas en un cronograma para su solución a largo plazo.

9 BCP business continuity plan

El Plan de Continuidad del Negocio, es un conjunto de estrategias y procedimientos diseñados para garantizar que una organización pueda seguir operando durante y después de un evento disruptivo, como desastres naturales, ciberataques o fallos tecnológicos.

ISO 22301 (Estándar Internacional): La norma ISO 22301 define el BCP como un "enfoque global y estructurado para prevenir y responder a posibles incidentes que interrumpan las actividades de negocio, asegurando la recuperación eficiente y el mantenimiento de la operatividad durante las crisis".

Gartner (Consultora tecnológica): Gartner describe el BCP como "un conjunto de prácticas organizacionales diseñadas para proteger y asegurar la continuidad de las operaciones empresariales ante eventos inesperados, minimizando el impacto en los procesos clave".

National Institute of Standards and Technology (NIST): El NIST describe el BCP como un "plan integral que incluye estrategias de prevención, recuperación y restauración para las actividades comerciales, asegurando que las funciones esenciales del negocio continúen operando en caso de una interrupción grave".

Business Continuity Institute (BCI): El BCI considera el BCP como "un enfoque disciplinado para planificar cómo una organización responderá a emergencias que puedan interrumpir las operaciones normales, con el objetivo de reducir al mínimo los efectos en las personas, los procesos, la infraestructura y la información".

En conclusión, actualmente en RCO no contamos con un plan formal de continuidad del negocio. Según el plan director de la empresa, se prevé que este se desarrolle en 2026. Sin embargo, considero que es crucial comenzar con el diseño e implementación de este proceso lo antes posible, ya que el Plan de Continuidad del Negocio es un documento dinámico que no solo aborda aspectos tecnológicos, sino también los procesos críticos del negocio. A pesar de ello, RCO ha decidido priorizar inicialmente el Plan de Recuperación ante Desastres (DRP).

10 DRP *Disaster recovery plan*

El DRP (Disaster Recovery Plan, o Plan de Recuperación ante Desastres) es un conjunto de procedimientos y estrategias diseñadas para recuperar los sistemas y datos de una organización después de un evento disruptivo, como un desastre natural, un ataque cibernético o un fallo tecnológico:

- ISO 22301 (Estándar Internacional): La ISO 22301 define el DRP como "un plan integral que detalla las acciones que una organización debe seguir para restaurar los sistemas de TI y las operaciones críticas después de un incidente o desastre, minimizando el impacto sobre los servicios y las funciones esenciales".

- National Institute of Standards and Technology (NIST): El NIST describe el DRP como "un conjunto de estrategias y procedimientos diseñados para permitir que una organización recupere sus sistemas de tecnología de la información (TI) y sus aplicaciones críticas en caso de una interrupción severa, asegurando la continuidad de las operaciones empresariales esenciales".

- Gartner (Consultora tecnológica): Gartner define el DRP como "un conjunto de procedimientos para recuperar las funciones tecnológicas de una organización después de un evento de desastre, cuyo objetivo es restaurar la operatividad de los sistemas de TI y minimizar el tiempo de inactividad para evitar la pérdida de datos y la disrupción de las operaciones comerciales".

- Business Continuity Institute (BCI): El BCI describe el DRP como "el conjunto de medidas y procedimientos implementados para garantizar la recuperación de las infraestructuras tecnológicas de una organización después de un evento disruptivo. Esto incluye el acceso a datos respaldados, la restauración de servicios de TI y la restauración de operaciones comerciales críticas".

En mi opinión, contar con un Plan de Recuperación ante Desastres (DRP) es fundamental para cualquier organización, ya que garantiza la restauración de los sistemas en caso de un desastre, sea del tipo que sea. En RCO, durante el ataque, no disponíamos de un DRP completo. Aunque existe un sitio alterno donde es posible restablecer algunos servicios, no se han considerado todos los servicios críticos. Además, no contamos con un DRP documentado ni oficial; el plan actual es empírico.

De acuerdo con el Plan de Dirección de Tecnologías de la Información, el diseño completo del DRP, que incluirá tanto la documentación como el hardware y software necesarios para asegurar su éxito, está programado para diciembre de 2024, mientras que su implementación se prevé para el segundo trimestre de 2025.

Capítulo 2

Descripción de la metodología empleada.

La metodología que seguimos para la recuperación acompañados de una compañía llamada NTT data la cual estaba contratada para ser nuestro equipo de respuesta a incidentes de seguridad fue de la siguiente manera:

- Análisis de Daños: Evaluamos cuantos servicios estaban detenidos.
- Planificación de la Recuperación: Desarrollamos un plan para abordar los daños y restaurar las operaciones. Es decir, restauración de sistemas, comunicación con partes interesadas, y la implementación de procesos de emergencia manuales.
- Implementación: Ejecutar el plan de recuperación, asignar recursos y coordinar acciones.
- Monitoreo y Evaluación: Supervisar el progreso y realizar ajustes según sea necesario.
- Revisión y Mejora Continua: Evaluar el proceso de recuperación para identificar lecciones aprendidas y mejorar futuros planes de contingencia.

Planeación o Cronología del proyecto.

			Inicio Proceso:	mar, 05/12/2023	
Lapso Estimado en días			Arranque Proyecto	mar, 05/12/2023	
				0	
TAREA	RESPONSABLE	PROGRESO	INICIO	FIN	DÍAS
FASE 1_Análisis de daños					
Cheklist de servicios criticos		100%	04/12/2023	05/12/2023	1
Cheklist de servidores infectados		100%	05/12/2023	05/12/2023	0
Cheklist de dispositivos infectados		100%	05/12/2023	05/12/2023	0
Consultar con expertos		100%	05/12/2023	05/12/2023	0
FASE 2_Planificación de la recuperación					
Identificación del tipo de ransomware		100%	05/12/2023	05/12/2023	0
Recoleccion de información del tipo de ranswomware		100%	05/12/2023	05/12/2023	0
Determinar el alcance del ataque		100%	05/12/2023	05/12/2023	0
Revision de copias de seguridad		100%	05/12/2023	06/12/2023	1
Decidir sobre el rescate que en este caso no pidieron		100%	06/12/2023	06/12/2023	0
FASE 3_Implementación					
Restauracion de sistemas críticos desde los respaldos de peaje		100%	06/12/2023	15/12/2023	7
Formateo de todos los equipos de peaje		100%	15/12/2023	15/12/2023	0
Reconexion de todo el cableado de peaje		100%	15/12/2023	26/12/2023	7
Restauracion de sistemas críticos desde los respaldos de corporativo		100%	26/12/2023	04/01/2024	7
Configuración de todos los equipos de corporativo		100%	04/01/2024	04/01/2024	0
Restauracion de sistemas críticos desde los respaldos de negocio		100%	04/01/2024	15/01/2024	7
Formateo de todos los equipos de negocio		100%	15/01/2024	15/01/2024	0
Reconexion de todo el cableado de negocio		100%	15/01/2024	18/01/2024	3
FASE 4_Monitoreo y Evaluación					
Se instalaron varios programas de monitoreo y seguridad		100%	18/01/2024	19/01/2024	1
Se monitorea el acceso de las vpn y se generan alertas		100%	19/01/2024	22/01/2024	1
Se monitorea los usuarios de acceso elevado con un pam		100%	22/01/2024	23/01/2024	1
Se monitoreo la red para asegurar que no habia un intruso		100%	23/01/2024	24/01/2024	1
Se realizo un escaneo en la red buscando anomalias		100%	24/01/2024	25/01/2024	1
FASE 5_Revisión y mejora continua					
Se esta subiendo los controles CIS a 3 para mejorar la seguridad		100%	25/01/2024	26/01/2024	1
Se instalo todo nuevo para asegurar que la red este limpia		100%	26/01/2024	29/01/2024	1
Se crearon playbooks para constante monitoreo de la red		100%	29/01/2024	30/01/2024	1
Se realizo un analisis de lecciones aprendidas		100%	30/01/2024	31/01/2024	1

Capítulo 3

Descripción de actividades

El martes 4 de diciembre del 2023 era un día de operaciones normales para RCO, la autopista funciona 24 horas, los 7 días de la semana, y contamos con personal de TI en cada caseta de 8 a.m. a 7 p.m. hay un técnico de guardia por la noche en la joya encargado de monitorear el tráfico en la pista y las alertas de peaje, en un horario de 10:00 p.m. a 7:00 a.m.

Estaba a punto de llegar a la sede corporativa el cual está ubicado en Guadalajara en Zapopan, cuando recibí una llamada a las 8:30 AM de Rodolfo Reyes (Encargado del sistema de peaje), su tono de desesperación me hizo saltar “Hemos sufrido un ataque”. Ante mi pregunta de dónde, me respondió que en Tepatitlán. Mi primer pensamiento fue que estábamos siendo atacados por los narcotraficantes en la caseta.

A medida que Rodolfo continuaba su relato, comprendí que se trataba de un ataque de ciberseguridad. Una de las computadoras de peaje en Tepatitlán, específicamente la de las cajeras encargadas de los cobros en la autopista, podemos observar la caseta en la figura 2 “Caseta de Tepatitlán”, presentaba un archivo de texto extraño y el sistema de cobro estaba funcionando de manera muy lenta. Rodolfo Reyes (Encargado del sistema de peaje) me informó que ya había alertado a Andrea Camaño, CISO, y a César Quiroz, director de Tecnología.

Figura 2 “Caseta de Tepatitlán”

04/12/2023, 09:00 AM: Andrea Camaño, CISO, instruyó a Rodolfo Reyes, encargado del sistema de peaje, a desconectar el enlace de internet y todos los equipos de la red en la figura 3 “Cables de red caseta Tepatitlán” podemos observar la cantidad de cables de red que no deberían desconectarse, sólo debió desconectar la energía eléctrica. Se aislaron las comunicaciones hacia internet entre las oficinas, las plazas de cobro y los carriles. Además, la jefa de operaciones de TI ordenó al coordinador de infraestructura que aislara el sistema que alberga las bases de datos y aplicaciones de RCO en La Joya, lo cual se llevó a cabo desconectando la red principal.

Figura 3 “Cables de red caseta Tepatitlán”

04/12/2023 11:00 AM Se traslada a Tepatitlán un analista de soporte y un analista de seguridad para examinar los primeros equipos infectados. Su primer paso fue identificar el archivo responsable de la infección. Durante la búsqueda de archivos maliciosos, durante la búsqueda de archivos maliciosos encontraron un archivo de texto denominado *AKIRA* “Figura 4 Imagen de equipo infectado”. Se envía el archivo al proveedor NTT data para que nos ayudara a confirmar si efectivamente se trababa del *ransomware AKIRA*.

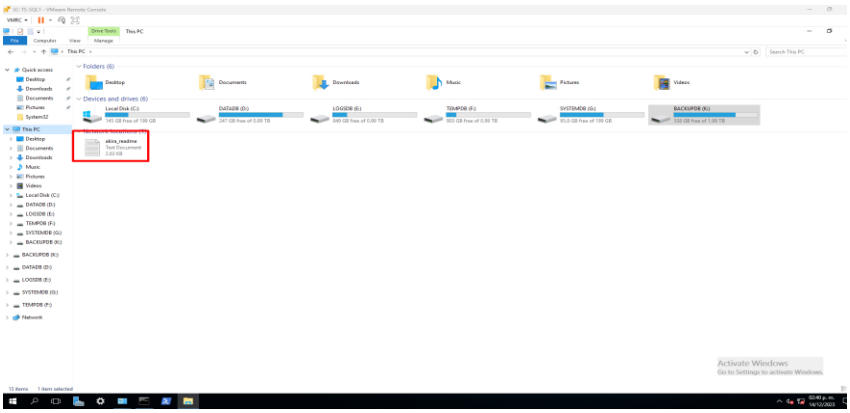


Figura 4 “Imagen de equipo infectado”

NTT DATA confirmó que se trata del *ransomware AKIRA* y nos proporcionó orientación sobre cómo detectar si algún equipo o servidor ha sido infectado. Los archivos afectados pueden identificarse por la extensión. Akira. Este virus encripta la información, impidiendo su lectura por cualquier software. Sin embargo, al realizar un análisis exhaustivo del equipo, nos dimos cuenta de que la información no estaba encriptada.

El primer paso fue intentar desinfectar el equipo. Sin embargo, al realizar un reinicio que era necesario para eliminar el virus descubrimos que, al volver a acceder a la computadora, la base de datos y toda la información se habían encriptado. Esto provocó la pérdida total de la información del equipo. Ante esta situación, Andrea Camaño (CISO) instruyó a toda la organización a no reiniciar ninguna computadora ni servidor.

04/12/2023, 12:00 PM: Se realiza un análisis de la situación actual del ataque y se evalúan las acciones necesarias a nivel del sistema de peaje para limpiar el virus.

El primer paso es analizar los servidores comprometidos. Para ello, es necesario conectarse a cada uno y revisarlos uno por uno. Estas actividades suelen requerir una hora de trabajo de dos ingenieros. Sin embargo, al intentar conectarse, los ingenieros encontraron que los servidores respondían con mucha lentitud.

Ante esta situación, se tomó la decisión, en conjunto con el equipo directivo, de restaurar los servidores críticos del sistema de peaje desde los respaldos. Esto incluye tres servidores centralizados y uno por plaza, sumando un total de 12 servidores para recuperar la operación de peaje. Además, hay 148 máquinas en los carriles, por lo que un equipo de técnicos se encargó de formatear todos los equipos y restablecer el respaldo en cada uno de ellos.

La verificación de cuántos equipos estaban comprometidos nos llevó un día y medio, debido a la lentitud de la red.

05/12/2023 09:00 PM Se determina el total de equipos comprometidos.

SERVIDORES:

- Centro de datos (Joya): 49.
- Plaza (Peaje): 9
- Plaza (videograbadores): 25
- Plaza (servidores de video continuo, Geo visión):48
- Servidores de Negocios: 9

PC, LAPTOP Y COMPUTADORA INDUSTRIAL (OT).

- Carriles y boleteras: 145.
- Puntos de Venta y computadoras de gerente tienda: 78
- Computadoras y PC's: 27

06/12/2023

Se convocó una reunión con el comité directivo para discutir la estrategia a seguir frente al grupo delictivo, dado que en el mensaje dejado en los equipos de cómputo mediante un archivo de texto, ver Figura 5 “Archivo de texto con mensaje de grupo delictivo”, amenazaba con no recuperar la información a menos que nos comunicáramos con ellos.

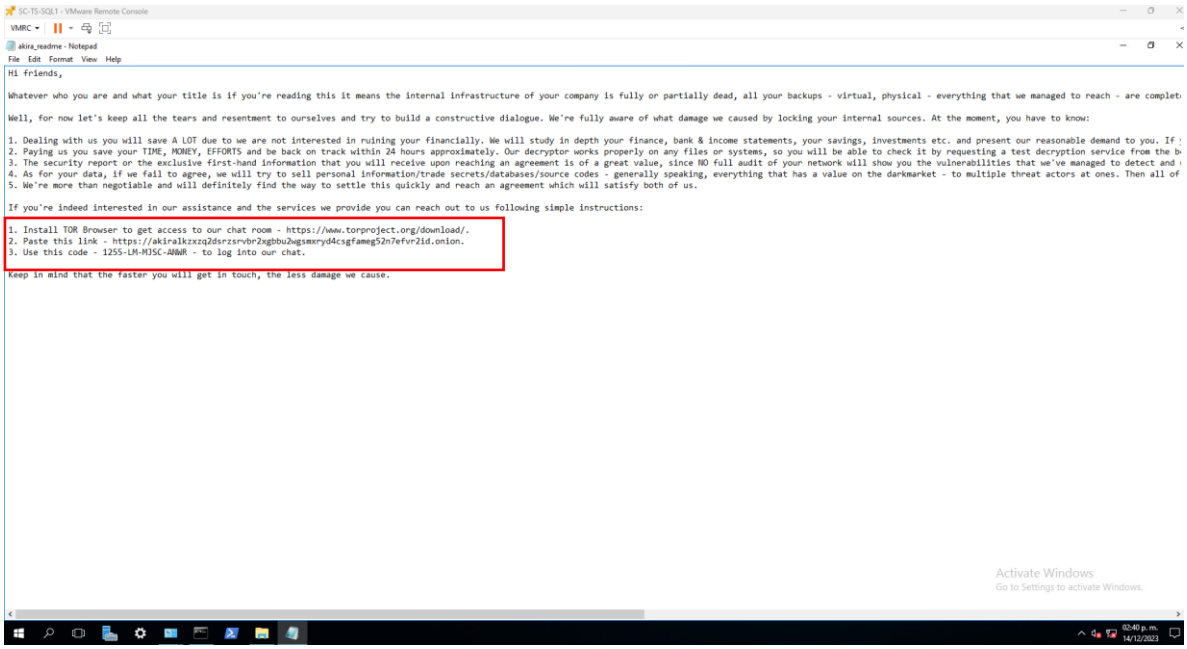


Figura 5 “Archivo de texto con mensaje de grupo delictivo”

El comité directivo decidió no contactar al grupo de *AKIRA* y, en caso de que se comunicaran con la empresa, se determinó que no se pagaría ningún rescate. Además, se realizó una revisión de la *deep web*, (conjunto oculto de sitios de Internet accesibles únicamente a través de navegadores especializados, utilizado para mantener la actividad en línea privada y anónima) en estos sitios, el grupo de *AKIRA* suele publicar la información de la empresa atacada con el fin de ejercer presión y que esta pague el rescate.

En esta misma reunión se realizó una lista de los sistemas críticos y la prioridad que se le daría a cada uno de ellos, quedando como prioridad 1 peaje, prioridad 2 sistemas corporativos, prioridad 3 negocios, prioridad 4 bodegas, prioridad 5 corporativos, prioridad 6 joya.

22/12/2023: Para este día todo el sistema había sido recuperado, para poder realizar todo este trabajo se requirieron 22 técnicos a lo largo de la autopista, ingeniero de servidores, ingeniero de redes, proveedores en la joya para recuperación de servidores, fue bastante retador coordinador a todas las personas, debíamos mandar ingenieros por ambos tramos de la autopista, autos, comida, gasolina. A estos equipos se les llamo bomberos durante esta incidencia. Ver figura 6 “Validaciones de seguridad de peaje”

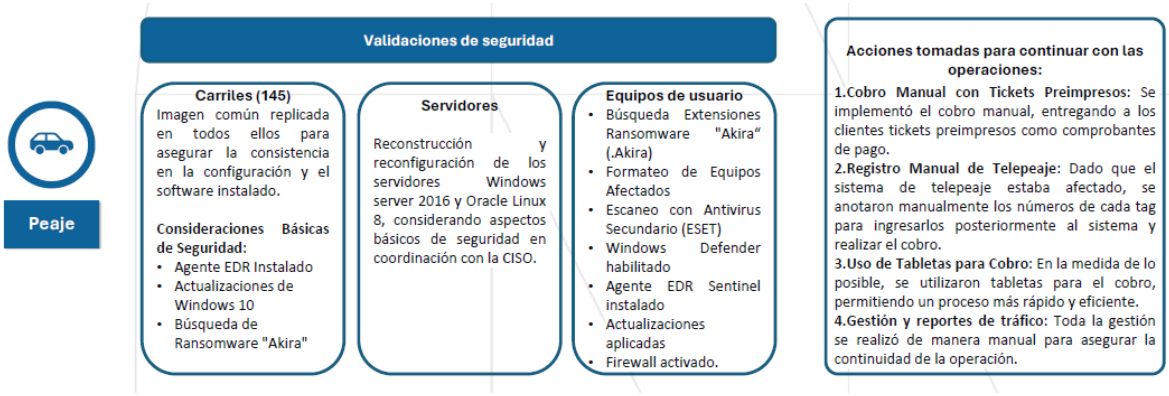


Figura 6 “Validaciones de seguridad de peaje”

Uno de esos días enviamos a dos ingenieros a Paníndicuaro, en Michoacán. Salieron a las 2 de la tarde de La Joya, en Zapotlanejo, y el viaje dura aproximadamente tres horas y media, por lo que debían llegar a su destino alrededor de las 5 p.m. Comencé a llamarlos a las 6 p.m., pero no obtenía respuesta de ninguno de ellos. Solicité ayuda al auxiliar vial, pero no lograron localizarlos. Luego llamé al encargado de la flota para rastrearlos por GPS. Para ese momento, ya estaba muy preocupada, ya que Michoacán es una zona que se evita de noche.

Afortunadamente, alrededor de las 8 p.m., finalmente me respondieron. Se habían perdido y tenían hambre, así que se detuvieron a comer en un puesto de tacos a lo largo del camino. Sentí un gran alivio al saber que estaban a salvo; es una gran responsabilidad enviar ingenieros a la ruta, y agradecí mucho que estuvieran bien.

Cabe mencionar que reconectar el cableado de red fue una tarea titánica, ya que los cables no estaban identificados. Normalmente, estos cables tienen números que indican dónde deben conectarse como se puede visualizar en la figura 7 “Identificación de cables de red”, pero en este caso, este trabajo aún no se había realizado en todos los sitios de la autopista. Por lo tanto, la identificación de los cables resultó ser un proceso arduo y que requirió mucha paciencia.

Figura 7 “Identificación de cables de red”

26/12/2023: Han pasado 22 días desde el ataque y todo el equipo está exhausto, habiendo trabajado jornadas de 16 horas diarias. La Navidad se acerca y aún no hemos recuperado los sistemas de la corporativo, lo que se ha vuelto una tarea urgente. La facturación hacia nuestros clientes no está disponible y no podemos posponerla más tiempo, al igual que los pagos a proveedores y otras operaciones esenciales. En una semana recuperamos todos los sistemas de corporativo y la conexión con España después de cumplir muchos requisitos. El 24 de diciembre nos fuimos a las 8 pm y el 25 de diciembre no trabajamos, para el 4 de enero todos los servidores y todas las computadoras de corporativo habían sido formateadas y estaban listas para operar. Breve resumen en Figura 8 “Recuperación y validaciones de seguridad”

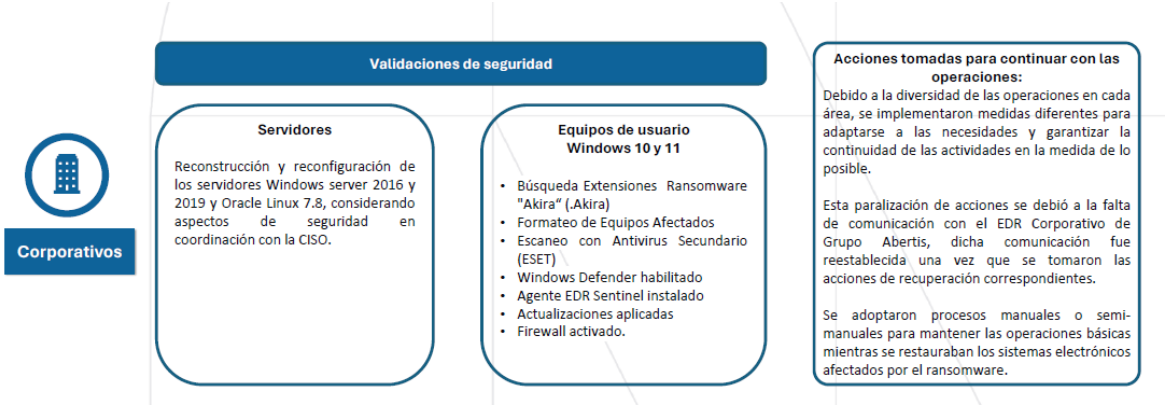


Figura 8 “Recuperación y validaciones de seguridad”

04/01/2024 En un sistema de autopistas, es fundamental contar con grabaciones de todas las casetas de peaje. Cuando un vehículo pasa por una caseta, hay sensores en el suelo y en el techo que determinan el tamaño del auto o camión que está realizando el pago. Los auditores revisan de manera aleatoria estos pagos por motivos de cumplimiento y en aquellos casos donde haya discrepancias entre lo cobrado y lo que detectó el sensor. Para el 4 de enero de 2024, el sistema de grabación ya estaba disponible.

5/01/2024: Los servicios auxiliares, que comprenden un conjunto de franquicias gestionadas por RCO, fueron de las últimas áreas en las que se concentraron los esfuerzos de recuperación y reactivación tras el incidente.

Estas franquicias incluyen una variedad de negocios y servicios, algunos de propiedad directa de RCO y otros operados bajo licencia de uso, que son fundamentales para complementar las actividades principales de la compañía y proporcionar valor añadido a los clientes. Se envió un equipo de ingenieros a todos los negocios para recuperar los servidores físicos, trasladarlos a La Joya, formatearlos y devolverlos a su localidad, todo en el transcurso de una semana. Además, contamos con la ayuda de dos ingenieros de nuestro proveedor IDRALL. Al mismo tiempo otro equipo de dos personas se dio a la tarea de preparar las nuevas computadoras para negocios, son 98 equipos. Resumen de equipos de negocios en Figura 8 “Recuperación y equipos de POS”

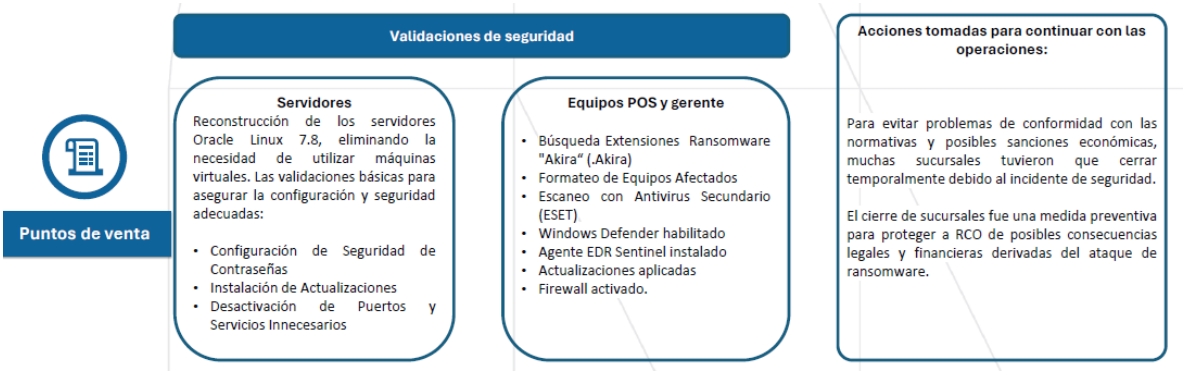


Figura 9 “Recuperación y equipos de POS”

11/01/2024 Se recupera el sistema de videograbación continua de peaje.

El resto de las computadoras y activos comprometidos se recuperaron en otras fechas entre el 04/12/2023 y el 19/01/2024.

18/01/2024: Una vez restaurada las operaciones, se realizó un análisis de lecciones aprendidas, utilizando como marco de referencia la versión 2.0 del NIST Cybersecurity Framework (*NIST National Institute of Standards and Technology CSF Cyber Security* Framework), Figura 10 “Marco de referencia NIST” El marco organiza las acciones y políticas de ciberseguridad en seis funciones clave: Gobierno, Identificar, Proteger, Detectar, Responder y Recuperar.

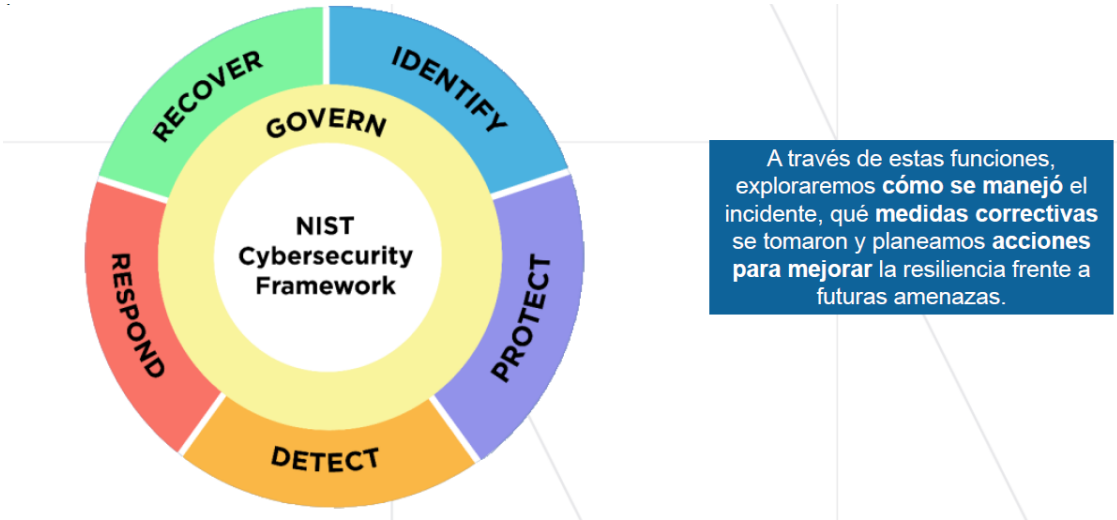


Figura 10 “Marco de referencia NIST”

NTT Data proveedor de RCO a cargo de la oficina de seguridad, nos ayudó a analizar las acciones inmediatas que deberían manejarse para proteger los activos contra amenazas futuras, todas estas actividades se realizaron entre el 4 de diciembre del 2023 y el 24 de enero del 2024.

1.- **Identificar**. Mantener el entorno tecnológico constantemente actualizado contribuye a reducir la posibilidad de vulnerabilidades identificadas. Al aplicar las correcciones proporcionadas por los fabricantes mediante actualizaciones, proteges de manera efectiva tus activos, lo cual realizamos en todos los activos que fueron recuperados, en nuestro caso, al momento del ataque los activos no estaban actualizados por lo que el riesgo a un ataque era mayor. Cabe mencionar que esta labor fue titánica ya que algunas casetas de peaje no cuentan con un internet de un ancho de banda lo suficientemente efectivo para realizar esta tarea, y en el site principal al estar actualizando todo al mismo tiempo hizo que colapsara la red, por lo que fue necesario duplicar el ancho de banda del enlace. Ver Figura 11 recomendaciones NTT data actualizaciones”

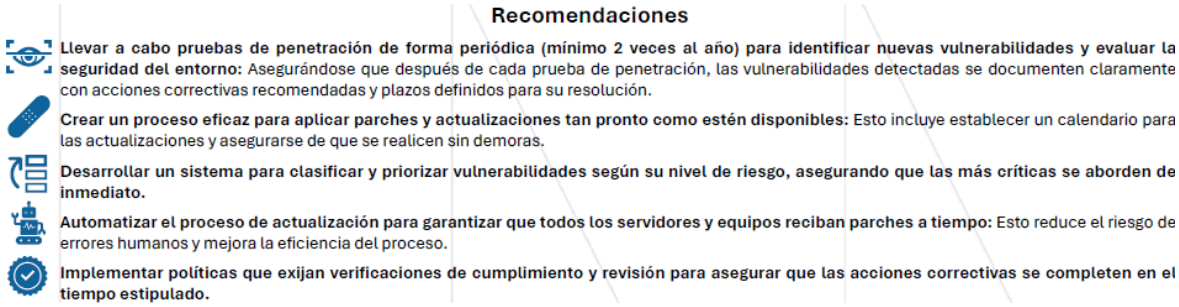


Figura 11 recomendaciones NTT data actualizaciones”

2.- **Identificar**. Tener un control de activos automatizado, facilita la respuesta ante incidentes, al tener un registro claro de los activos afectados y su estado. Al momento del incidente se llevó a cabo un registro riguroso de cada uno de los activos con una herramienta de descubrimiento, un control de activos sólido es crucial para la seguridad, la eficiencia y la gestión efectiva de recursos. Las casetas de peaje tienen un sistema de cobro muy sensible por lo que cada software que se necesite instalar debe ser probado antes de la instalación para asegurar que no haya afectación en producción. Este software nos permite ver toda la información de software y hardware del equipo, Ver Figura 12 “Control de activos Sistema Fresh Service”.

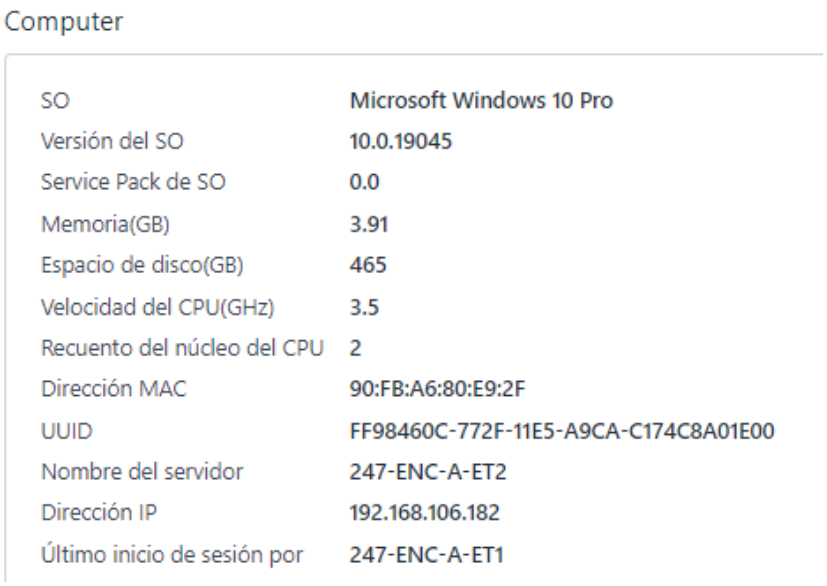


Figura 12 “Control de activos Sistema Fresh Service”

Además de las actualizaciones se activó el *BitLocker* en todos los equipos con el fin de tener cifrado el disco de las computadoras, con este cifrado garantizamos que la información no se pueda leer, aunque te roben el equipo. Ver figura 13 “***Bitlocker”.***

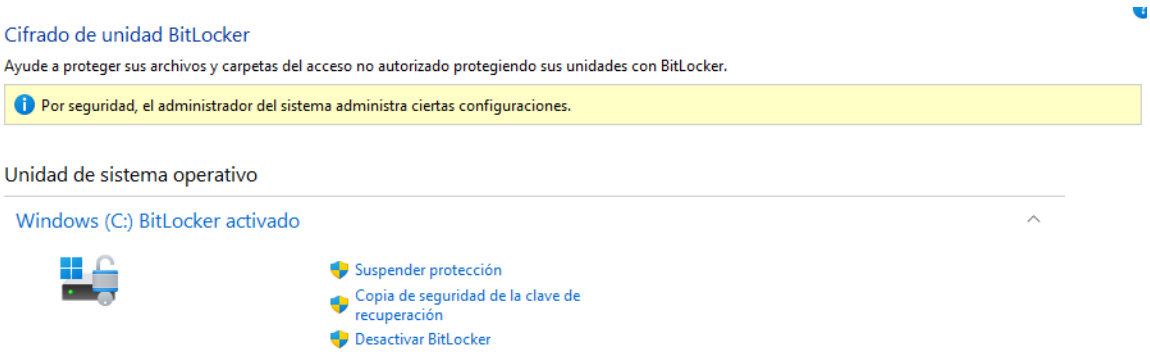


Figura 13 “Bitlocker”

3.- **Proteger**. Contar con un antivirus que integre inteligencia artificial y funcione como *EDR (Endpoint Detection and Response*) es fundamental, ya que esta herramienta proporciona monitoreo y análisis continuo de los *endpoints* y la red. RCO disponía de una solución *EDR*, pero lamentablemente no estaba instalada en todos los dispositivos. Si hubiera estado implementada en todos ellos, habría podido detectar y neutralizar el ransomware, dado que su objetivo es identificar, detectar y prevenir amenazas avanzadas de manera más efectiva. Uno de los desafíos a los que nos tuvimos que enfrentar es que las malas prácticas que se tenían en *RCO*, por ejemplo, enviar un ping, hace que el *EDR* bloquee el equipo y lo saque de la red, por lo que tuvimos que desaprender muchas malas prácticas. Se configuro una alerta para que nos envié notificación si algún equipo se fue a cuarentena por falta de actualización del antivirus, además de que el *SOC* está en continuo monitoreo.

4.- **Proteger**. Mantener un acceso seguro a la red empresarial mediante una VPN (Red Privada Virtual) es crucial. Durante el incidente, además de los múltiples problemas causados por el ataque, se sumó otro: el daño al switch principal del centro de datos. Esta avería dificultó la identificación precisa de cuántos servidores estaban infectados. Como una mejora se implementó una nueva VPN (Red privada virtual) tras el daño sufrido por el switch principal. Se creó una red completamente nueva, y esta VPN está monitoreada por el SOC (Centro de Operaciones de Seguridad). En caso de detectar comportamientos inusuales, se envían alertas al equipo de seguridad y al equipo de operaciones de Tecnologías de la Información. Ver figura 14 “VPN Fortinet”. Adicional todos los usuarios de privilegios elevados para poderse conectar a administrar cualquier dispositivo deben conectarse a través de un doble factor de autenticación de Microsoft. Ver figura 14 “Microsoft Autenticator”.

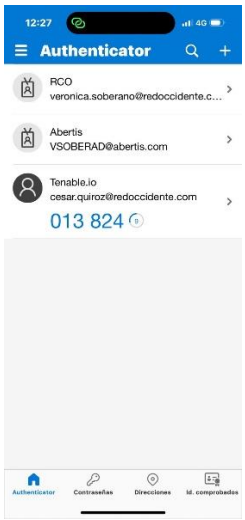


Figura 14 “Microsoft Autenticator”

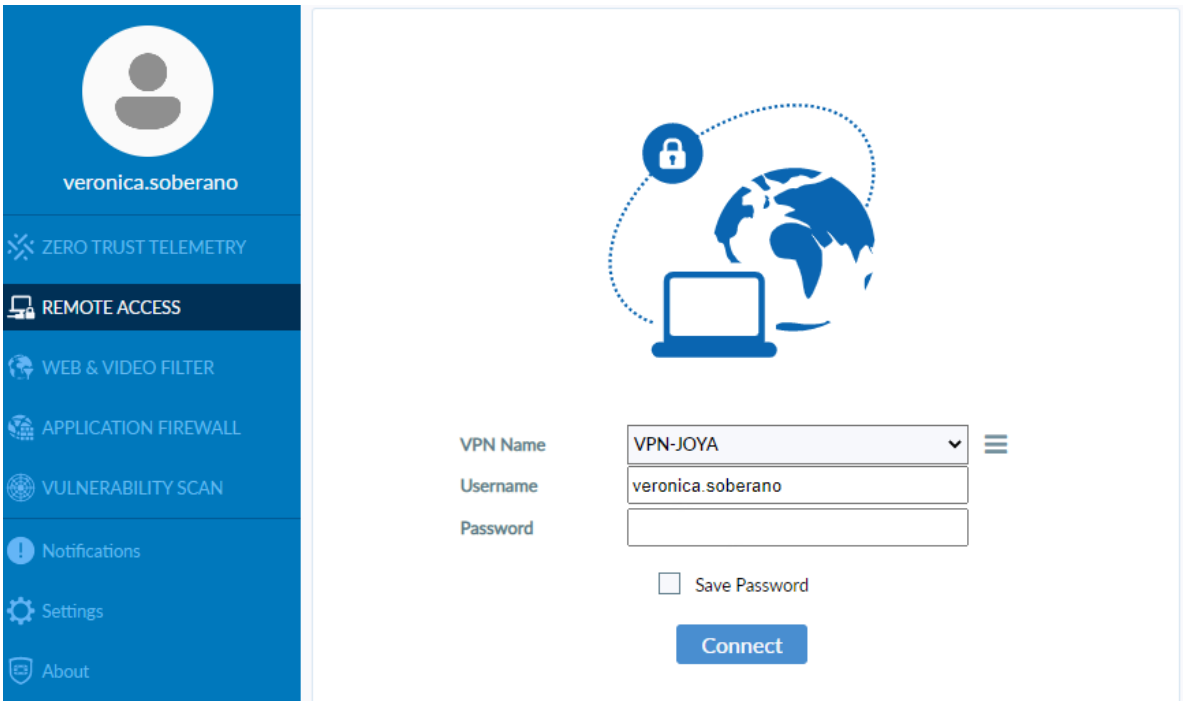


Figura 15 “VPN Fortinet”

5.- **Proteger.** Implementar una herramienta de soporte segura no solo protege a tus usuarios, sino que también ofrece múltiples beneficios para tu negocio. En RCO, ya contábamos con una herramienta segura para conexión remota, pero no estaba instalada en todos los equipos. Como parte de una mejora, se realizó la instalación en aproximadamente 600 dispositivos durante la incidencia. A partir de ahora, esta herramienta se instalará en cada dispositivo antes de ser entregado al usuario final, garantizando así un soporte más eficiente y seguro. Ver figura 16 “Logmein”.

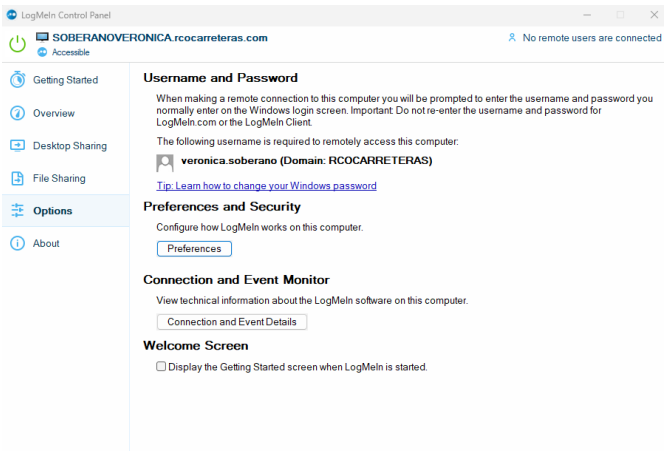


Figura 16 “Logmein”

6.- **Proteger**. Es fundamental mantener una gestión y control efectivo de todos los super usuarios, preferiblemente mediante una herramienta de Gestión de Accesos Privilegiados (PAM). Durante el incidente, la implementación de la herramienta PAM estaba en proceso de instalación y configuración, lo que permitió a los atacantes acceder a la red a través de un superusuario del área de Tecnologías de Información. Actualmente, contamos con una herramienta PAM que es monitoreada por el SOC las 24 horas del día, los 7 días de la semana. Esta herramienta genera alertas en caso de modificaciones en cuentas de administrador, como cambios de contraseña, bajas o activaciones.

Todos los usuarios administradores, así como los proveedores, acceden a la administración de dispositivos a través de la herramienta PAM, lo que permite tener video y registro de todas las acciones realizadas durante cada conexión.

Durante el incidente, el servidor donde estaba configurada la herramienta PAM fue infectado debido a la falta de un antivirus actualizado. Como resultado, se perdieron seis meses de trabajo y fue necesario recuperar toda la configuración en un plazo de dos meses, involucrando a seis ingenieros para lograrlo en un tiempo récord. Ver figura 17 “Herramienta PAM”.

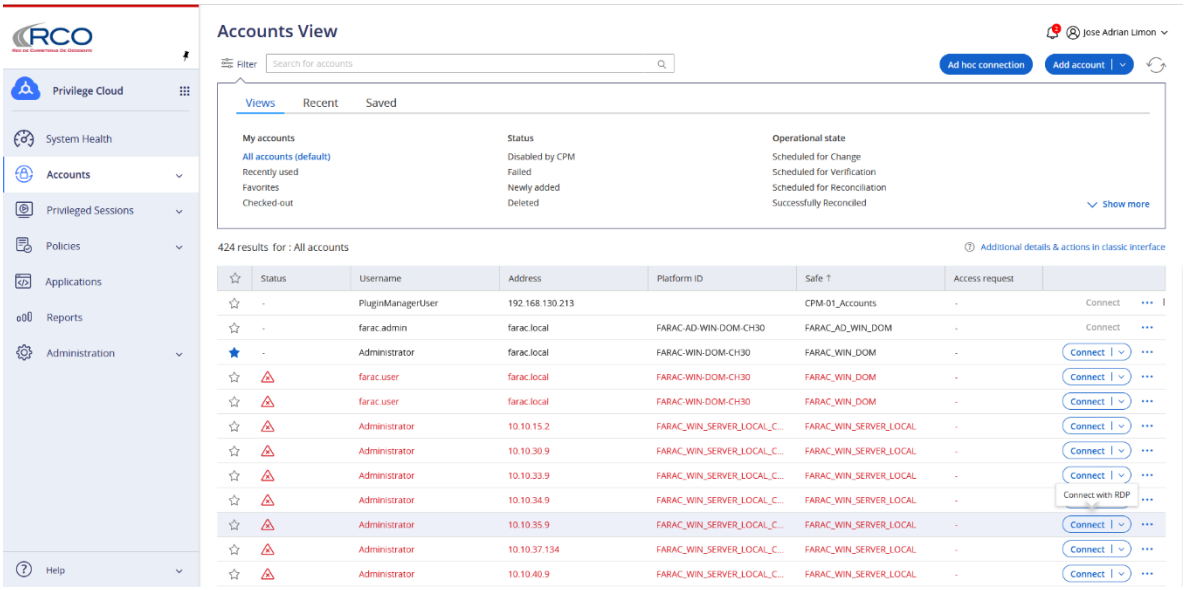


Figura 17 “Herramienta PAM”

7.- **Gobierno**. Se estableció una política de software autorizado para garantizar que las herramientas de seguridad se instalen en todos los nuevos activos y para prevenir la instalación de software no autorizado, esto se realizó de manera emergente más adelante haremos énfasis en la importancia de la documentación y comunicación de políticas y procedimientos a toda la organización. Ver Figura 18 “Listado de software autorizado”. NTT data nos realizo las siguientes recomendaciones que pueden ver en la Figura 19 “

Figura 18 “Listado de Software autorizado”

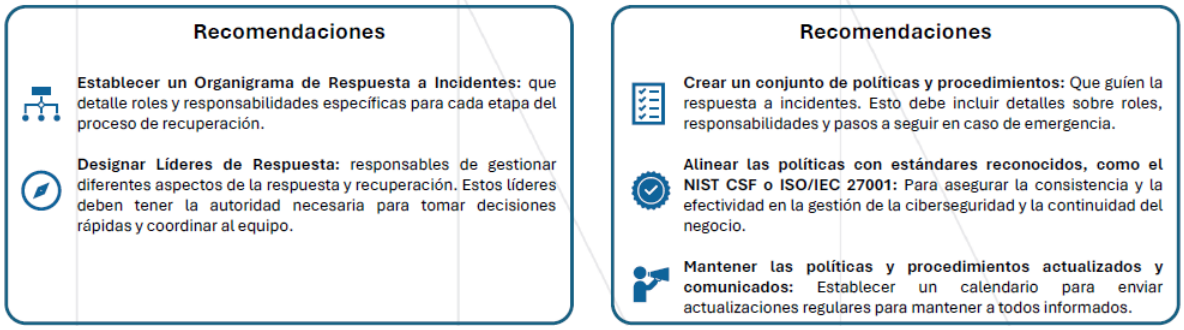


Figura 19 “Recomendaciones políticas y procedimientos”

8.- **Proteger**. Hay que asegurar que en la red no existan anomalías. Es decir, se realizó un escaneo de la red con una herramienta de *pentest* que es una técnica de ciberseguridad que consiste en simular un ataque a un sistema informático para detectar vulnerabilidades y prevenir ataques externos, con esta prueba pudimos verificar que todos los puertos estuvieran cerrados y únicamente los permitidos estuvieran abiertos.

25/01/2024 RCO está bajo la supervisión de un grupo corporativo llamado Abertis, con sede en España. Cada unidad de negocio a nivel mundial cuenta con un CISO local, quien mantiene una línea de reporte directa con el CISO de Abertis. La Ciso global viajo a Guadalajara con un proveedor llamado *one esecurity* el cual es un especialista líder en el mercado en detección de amenazas, análisis forense digital y respuesta a incidentes.

26/01/202

One esecurity nuestro proveedor de SOC (Centro de operaciones de seguridad) y NOC (Network Operation Center), solicito muestras del virus o algunos servidores infectados, cabe mencionar que si se tenían servidores infectados pero la operación se había caído una semana antes a la llegada del proveedor, debido a que no podía sostener todos los servidores en mi ambiente virtual operativo, por lo que el proveedor no pudo acceder a logs e información importante para un análisis forense, con la poca información que pudieron obtener durante 15 días llegaron a la conclusión que el ataque se llevó a cabo mediante la VPN obteniendo las credenciales de un usuario administrador de TI, con el cual pudieron entrar al directorio activo de IT (Tecnologías de información) y de ese servidor pudieron ingresar a la red OT (Tecnología operativa)

Una vez concluido el en análisis forense teníamos aun muchas preguntas. Por ejemplo, ¿Por qué ningún grupo se adjudicó el ataque? ¿Por qué no se publicó información de la empresa a pesar de que pudieron acceder a parte de ella? Estas preguntas no pudieron ser respondidas. Lo que debíamos hacer es prevenir y seguir las recomendaciones que no realizaron los distintos proveedores, iniciaremos con el monitoreo, por lo que el SOC (*Security Operation Center*) se volvió crucial.

A continuación, algunas de las recomendaciones de Abertis para el SOC *(Security Operation Center*) Figura x “Detección casos de uso” Dependiendo de la configuración de un caso de uso puedes detectar actividad sospechosa de un usuario, limitar los intentos de acceso, detectar escalamiento de contraseñas de administrador, etc. Puedes observar ejemplos de casos de uso en la figura 20 “Ejemplos de casos de uso”

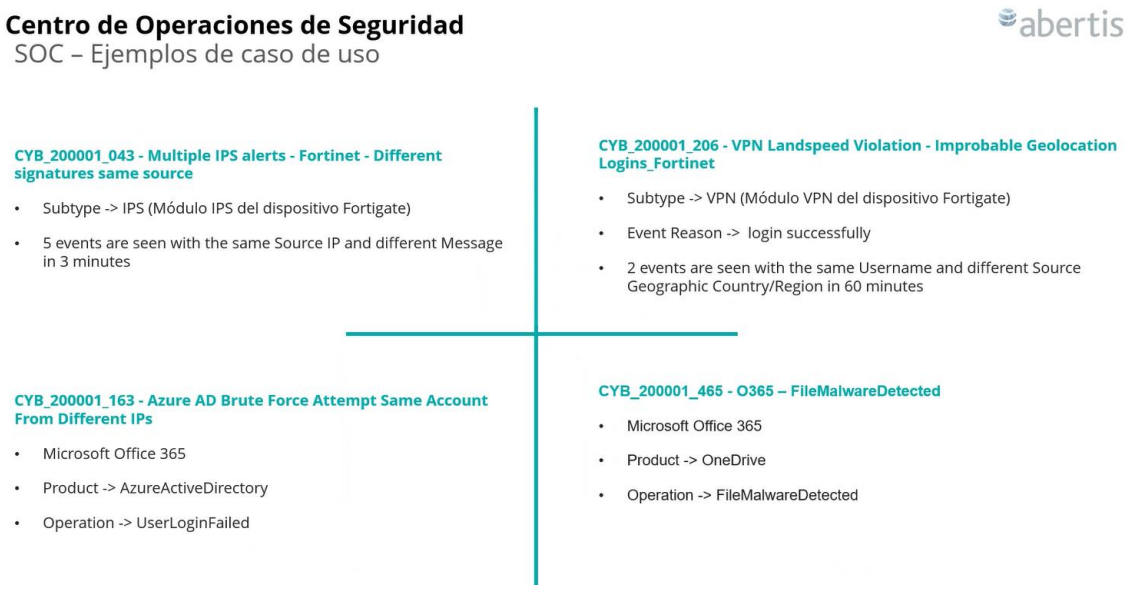


Figura 20 “Ejemplo de caso de uso”

La revisión de logs de manera permanente permite encontrar anomalías y problemas permitiendo resolver dichos problemas con la mayor eficiencia posible, la gestión de eventos se debe puede realizar de las siguientes fuentes, Figura 21 “Gestión de eventos”

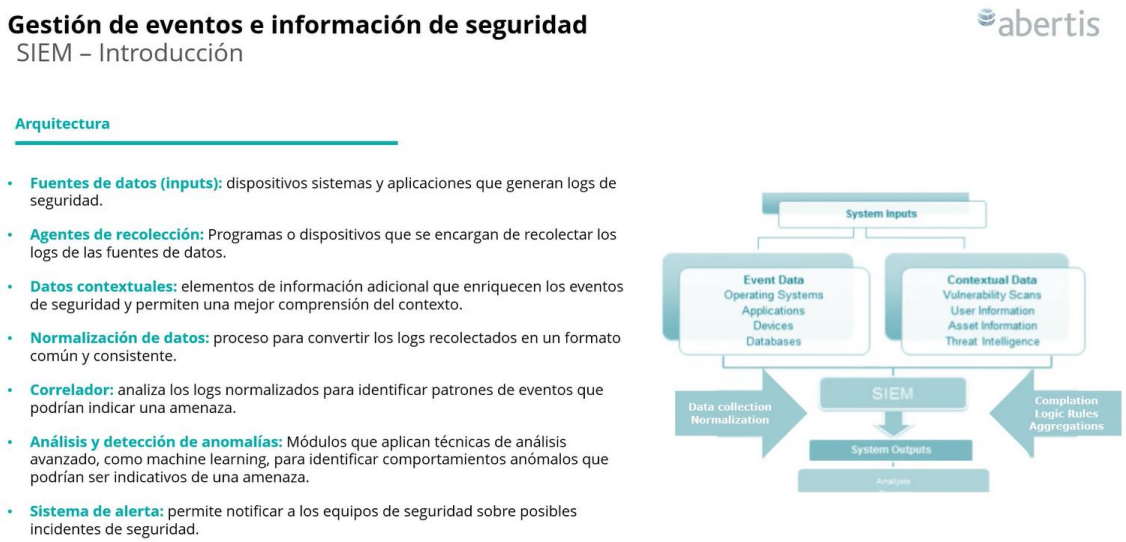


Figura 21“Gestión de eventos de seguridad”

Lecciones aprendidas

Siguiendo las recomendaciones de Abertis, se pudo mejorar al SOC de RCO y estos son los reportes que nos envían actualmente. RCO realizo un manual de operaciones con el cual el SOC (Security Operation Center) puede identificar y asignar los incidentes de acuerdo el impacto considerado en el manual. Figura x “Eventos de seguridad del mes”

1. Resumen de Actividades

Durante la semana se registraron un total de **40 eventos de seguridad** categorizados de **bajo** impacto de acuerdo con el manual de operaciones establecido por RCO**:**

	Eventos de seguridad revisados.	Incidentes de seguridad
Total	**43**	**0**
Bajo	43	-
Medio	-	-
Alto	-	-
Crítico	-	-

Figura 22 “Eventos de seguridad del mes”

2. Estado de salud Sentinel One.

El objetivo de este apartado es mostrar la salud de los agentes instalados de la herramienta de *Sentinel One*, para lo cual, se tomarán en cuenta los siguientes valores:

● Versión del agente.
El KPI recomendado es tener en una versión actualizada a más del 90% del total de agentes instalados. Por lo tanto, para que el agente sea considerado como actualizado la condición es que el agente sea al menos dos versiones menores a la más reciente y que además sea en su segundo dígito de izquierda a derecha sea mayor a 3.

Consideraciones:
La versión más reciente para los siguientes sistemas operativos es Figura X “Versiones sistemas operativos RCO”:

Sistema operativo	Versión del agente	Versión mínima aceptable
Windows	23.4.5.337	21.3.x.x
MacOs	24.2.2.7632	22.3.x.x
Linux	24.2.2.20	22.3.x.x

Figura 23 “Versiones sistemas operativos RCO”

3. Estado de salud Sentinel One.

Los equipos decomisados son aquellos equipos que por falta de actividad se detiene el agente del antivirus, estos equipos se verifican para revisar porque no presentan actividad. Figura X “Equipos decomisados”

Fecha y hora	Nombre del equipo	Tipo
Oct 13, 2024 18:49:52	Biometricos	Automatico
Oct 13, 2024 18:49:52	R0ci0LMartinez	Automatico
Oct 12, 2024 20:42:39	XLC1104	Automatico
Oct 11, 2024 04:43:04	CESAR-ALCARAZ	Automatico
Oct 08, 2024 12:46:27	EMA-RODRIGUEZ	Automatico

Figura 24 “Equipos decomisados”

4. Estado de las integraciones en Stellar Cyber.

4.1 Conectores

Un **conector** es un componente que permite la integración de diversas fuentes de datos y sistemas externos con la plataforma de seguridad de *Stellar Cyber* que nos permiten en unos casos responder y/o colectar. Figura 25 “Estado de conectores Stellar Cyber”.

Nombre	Herramienta	Healt check	Mas detalles
Americas-A	Fortigate	Saludable	
DOMINIO FARAC	Active Directory	No saludable	Se registra un error en la cuenta asociada al conector
DUO RCO	Duo Security	Saludable	
FGT-ANTIGUA	Fortigate	Saludable	
FGT-CENTRAL-ABASTOS	Fortigate	Saludable	
FGT-COPANDARO	Fortigate	Saludable	
FGT-CORE	Fortigate	Saludable	
FGT-ECUANDUREO	Fortigate	Saludable	
FGT-ENCARNACION	Fortigate	Saludable	
FGT-JALOSTOTITLAN	Fortigate	Saludable	

4. controles CIS.

Tener controles CIS (*Center for Internet Security*) son un conjunto de buenas prácticas y controles de seguridad que ayudan a las empresas a mejorar su postura de Ciberseguridad. Los cuales son evaluados por el departamento de seguridad de la información global de Abertis. Esta evaluación es trimestral, lo que hacen es pedirnos evidencia de cada uno de los controles, revisan de manera detallada cada una de esa evidencia y nos evalúan cada control con un puntaje del 1 al 5 donde 5 es el máximo puntaje y debemos tener 3 como mínimo para tener una evaluación óptima para Abertis, acaban de realizar la evaluación de octubre y estos fueron los resultados. El nivel medio de madurez de RCO ha incrementado de 2,83 a 3,37

durante Q3 2024. Más que tener el puntaje de 3 la lección aprendida es, que tener los controles nos ayudan a proteger a RCO de una variedad de amenazas cibernéticas. En la tabla x “Controles Cis” podemos observa el nivel de madurez que RCO en las 18 mejores prácticas desarrolladas por el *Center for Internet Security (CIS).*

Subcontrol ID	Control title	Previous maturity level	Current maturity level	Final maturity level
1.1	Utilize an Active Discovery Tool	1,5	4	3
2.1	Maintain Inventory of Authorized Software	1	4	4
2.2	Ensure Software is Supported by Vendor	2	4	4
2.10	Physically or Logically Segregate High Risk Applications	3	4	4
3.1	Run Automated Vulnerability Scanning Tools	2	4	4
3.2	Perform Authenticated Vulnerability Scanning	2	4	4
3.3	Protect Dedicated Assessment Accounts	3	4	4
3.4	Deploy Automated Operating System Patch Management Tools	1	4	4
3.5	Deploy Automated Software Patch Management Tools	1	4	4

3.6	Compare Back-to-back Vulnerability Scans	1	4	2
3.7	Utilize a Risk-rating Process	2	3	3
4.2	Change Default Passwords	3	4	4
4.3	Ensure the Use of Dedicated Administrative Accounts	3	4	4
4.5	Use Multifactor Authentication For All Administrative Access	1	4	4
4.6	Use of Dedicated Machines For All Administrative Tasks	3	4	4
5.1	Establish Secure Configurations	2	4	3
6.1	Utilize Three Synchronized Time Sources	1	4	4
6.6	Deploy SIEM or Log Analytic tool	2	4	4
7.1	Ensure Use of Only Fully Supported Browsers and Email Clients	3	4	4
7.4	Maintain and Enforce Network-Based URL Filters	3	4	4
7.5	Subscribe to URL-Categorization service	3	4	4
7.7	Use of DNS Filtering Services	1	4	4

7.10		Sandbox All Email Attachments	3	4	4
8.7		Enable DNS Query Logging	3	4	4
8.8		Enable Command-line Audit Logging	3	4	4
9.1		Associate Active Ports, Services and Protocols to Asset Inventory	1	4	1
9.2		Ensure Only Approved Ports, Protocols and Services Are Running	3	4	3
9.3		Perform Regular Automated Port Scans	3	4	4
9.4		Apply Host-based Firewalls or Port Filtering	3	4	4
9.5		Implement Application Firewalls	3	4	4
10.4		Ensure Protection of Backups	3	4	4
10.5		Ensure Backups Have At least One Non-Continuously Addressable Destination	3	4	4
11.2		Document Traffic Configuration Rules	1	4	2
11.5		Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	3	4	4

11.7	Manage Network Infrastructure Through a Dedicated Network	3	4	4
12.1	Maintain an Inventory of Network Boundaries	3	4	4
12.5	Configure Monitoring Systems to Record Network Packets	1	4	4
12.7	Deploy Network-Based Intrusion Prevention Systems	3	4	4
13.4	Only Allow Access to Authorized Cloud Storage or Email Providers	3	4	4
13.6	Encrypt the Hard Drive of All Mobile Devices.	2	3	3
14.2	Enable Firewall Filtering Between VLANs	3	4	4
14.4	Encrypt All Sensitive Information in Transit	4	4	2
16.2	Configure Centralized Point of Authentication	3	4	4
16.4	Encrypt or Hash all Authentication Credentials	3	4	4
16.5	Encrypt Transmittal of Username and	3	4	2

		Authentication Credentials			
16.10		Ensure All Accounts Have An Expiration Date	3	4	4
16.11		Lock Workstation Sessions After Inactivity	3	4	4
16.12		Monitor Attempts to Access Deactivated Accounts	1	4	4
18.10		Deploy Web Application Firewalls (WAFs)	1	4	4
19.1		Document Incident Response Procedures	3	4	3,5
19.2		Assign Job Titles and Duties for Incident Response	3	4	3,5
19.3		Designate Management Personnel to Support Incident Handling	3	4	3,5
19.4		Devise Organization-wide Standards for Reporting Incidents	3	4	3,5
19.5		Maintain Contact Information For Reporting Security Incidents	3	4	3,5
19.6		Publish Information Regarding	3	4	3,5

		Reporting Computer Anomalies and Incidents			
19.8		Create Incident Scoring and Prioritization Schema	1	4	3
20.2		Conduct Regular External and Internal Penetration Tests	3	4	4
20.3		Perform Periodic Red Team Exercises	1	4	3
20.4		Include Tests for Presence of Unprotected System Information and Artifacts	1	4	4
20.5		Create Test Bed for Elements Not Typically Tested in Production	1	4	N/A
20.6		Use Vulnerability Scanning and Penetration Testing Tools in Concert	3	4	4
20.7		Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards	1	4	4
20.8		Control and Monitor Accounts Associated with Penetration Testing	1	4	4

CP.1	SOC incidents	2	4	4
CP.4	BCP/DRP	1	2	2
CP.5	User access	2	4	4

Tabla 1 “Controles *CiS*”

5. Encriptación de respaldos.

Una buena práctica es calendarizar los respaldos de la información crítica y, de manera regular realizar pruebas de recuperación de estos. En el caso de RCO se trabajó en tener los respaldos encriptados, los cuales se realizan con herramienta de *veeam backup* y las pruebas de recuperación se realizan de manera trimestral por nuestro proveedor de mantenimiento de servidores Intecfra proveedor de mantenimiento de servidores, anexo resultados de la prueba. Cabe mencionar que estos respaldos se realizan en frio, es decir, están fuera de línea totalmente inaccesibles. Figura 26 “Pantalla del sistema de *veeam backup*” en esta pantalla podemos observar que los respaldos están encriptados por *default*.

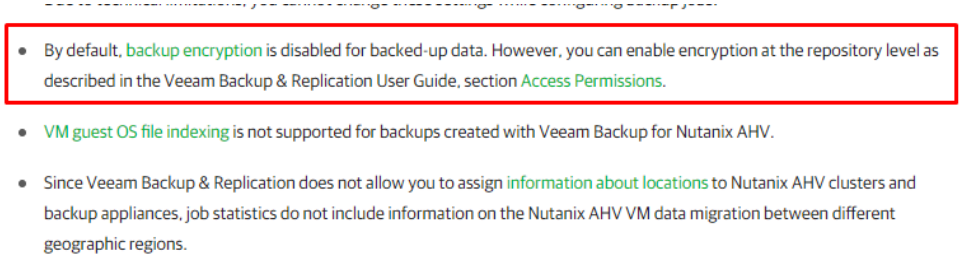


Figura 26 “Pantalla del sistema de *veeam backup”*

Prueba de restauración, servidor inmutable.

Figura 27 “Pantalla de veeam backup”. Se realiza la prueba con 3 respaldos aleatorios.

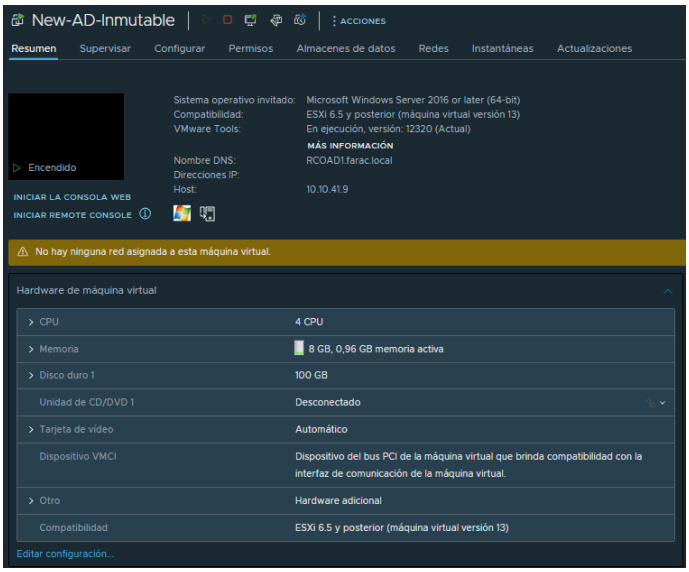


Figura 27 “Pantalla de veeam backup”.

- Servidor Directorio Activo Farac “New-AD” (IP 10.10.50.1)
- Como se muestra en la Imagen Figura 28 “Veeam Backup restore” el respaldo que se restauro es full.

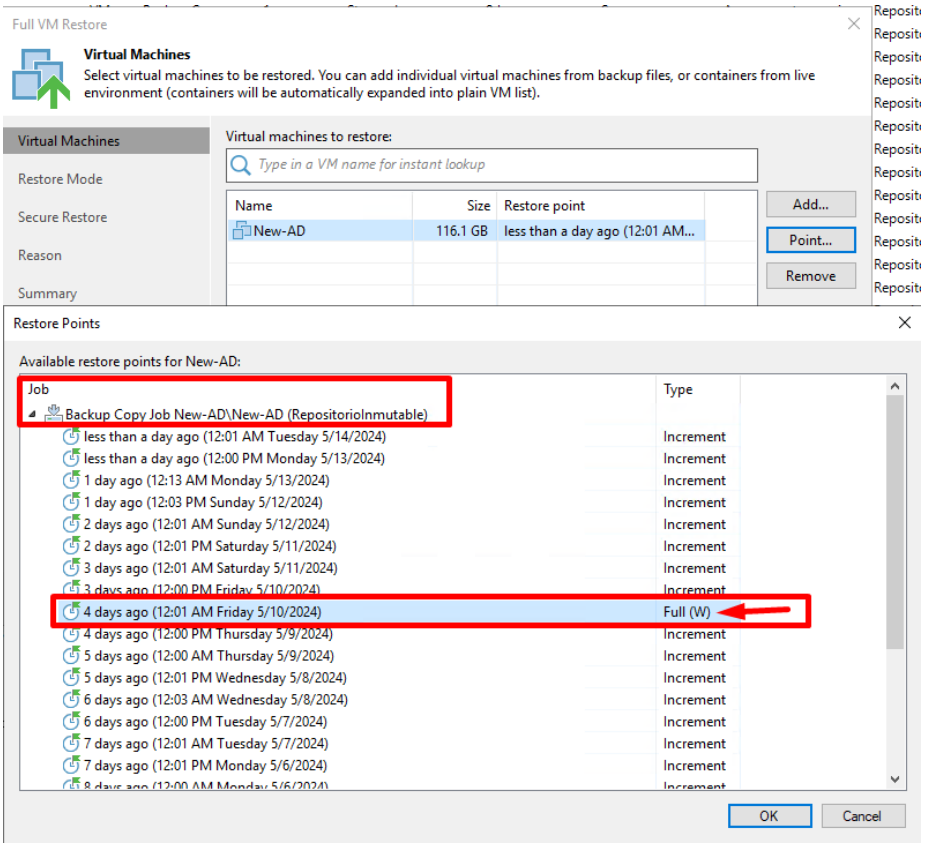


Figura 28 “Veeam Backup restore”

7. Assesment de 5 controles

Por parte de Abertis, se realizó un *assesment* de seguridad de 5 controles, por un proveedor llamado Innotec. Para realizar este *assesment* se le proporciono al proveedor acceso a un servidor y se le crearon usuarios de correo y de VPN. En la Figura 29 “Controles revisados por Innotec” podemos revisar el objetivo de este *assesment*.

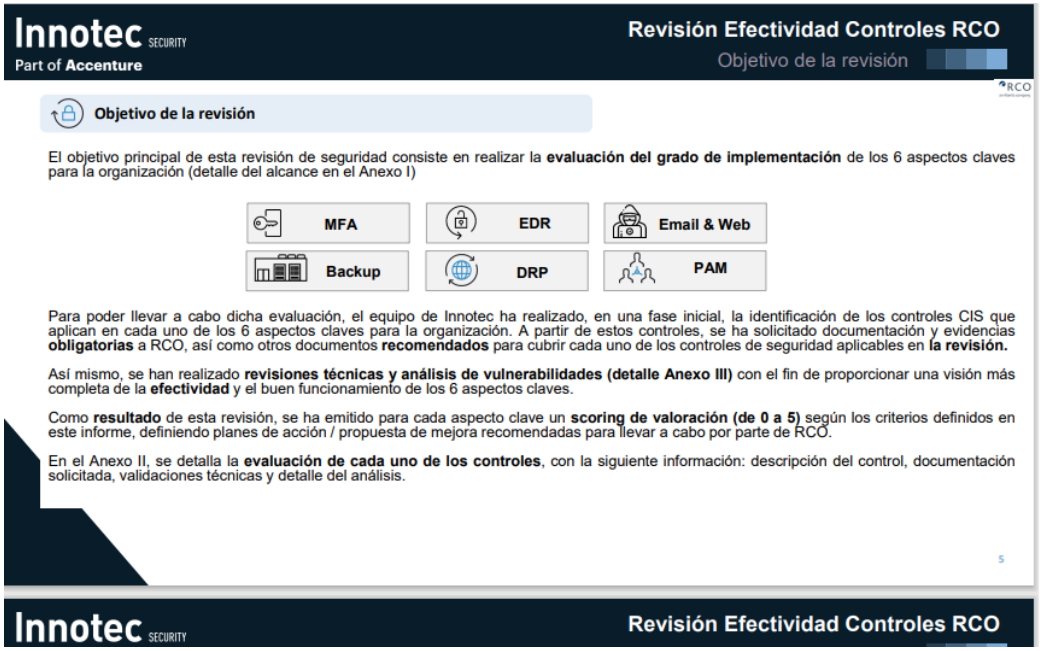


Figura 29 “Controles revisados por Innotec”

El objetivo de Abertis es evaluar el nivel de madurez de estos controles, los cuales se evaluaron como se describe en la Figura 30-31 “Criterios de Evaluación”

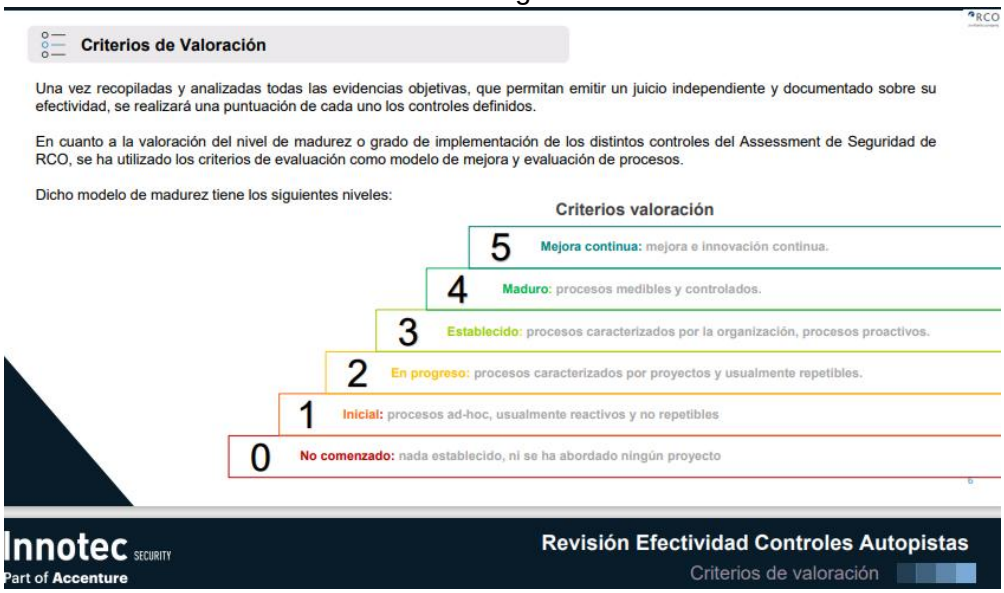
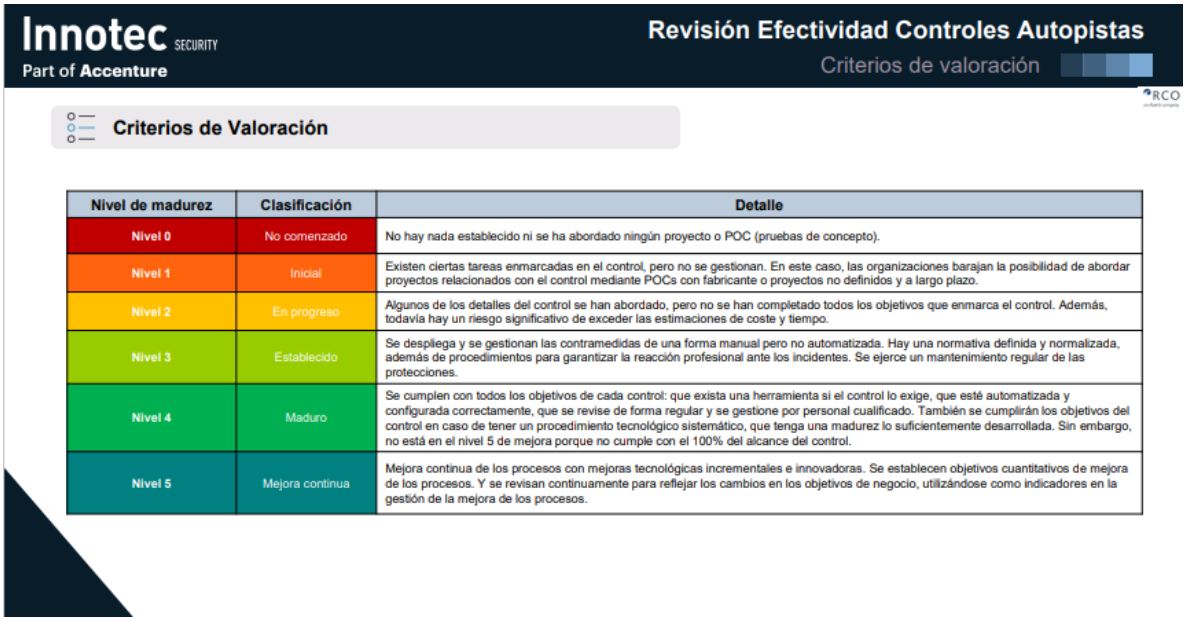


Figura 30 “Criterios de Evaluación”



Nivel de madurez	Clasificación	Detalle
Nivel 0	No comenzado	No hay nada establecido ni se ha abordado ningún proyecto o POC (pruebas de concepto).
Nivel 1	Inicial	Existen ciertas tareas enmarcadas en el control, pero no se gestionan. En este caso, las organizaciones barajan la posibilidad de abordar proyectos relacionados con el control mediante POCs con fabricante o proyectos no definidos y a largo plazo.
Nivel 2	En progreso	Algunos de los detalles del control se han abordado, pero no se han completado todos los objetivos que enmarca el control. Además, todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.
Nivel 3	Establecido	Se despliega y se gestionan las contramedidas de una forma manual pero no automatizada. Hay una normativa definida y normalizada, además de procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular de las protecciones.
Nivel 4	Maduro	Se cumplen con todos los objetivos de cada control: que exista una herramienta si el control lo exige, que esté automatizada y configurada correctamente, que se revise de forma regular y se gestione por personal cualificado. También se cumplirán los objetivos del control en caso de tener un procedimiento tecnológico sistemático, que tenga una madurez lo suficientemente desarrollada. Sin embargo, no está en el nivel 5 de mejora porque no cumple con el 100% del alcance del control.
Nivel 5	Mejora continua	Mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora de los procesos. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.

Figura 31 “Criterios de Evaluación”

De los seis controles revisados, RCO se encuentra en el nivel 3. En cuanto al respaldo, durante la revisión estábamos en proceso de migrar de la plataforma de virtualización *Veeamware* a *Nutanix*, lo que resultó en un nivel 2 para ese control. Sin embargo, actualmente ya ha alcanzado el nivel 3. Respecto al Plan de Recuperación ante Desastres (DRP), aún no está completo, pero su implementación está programada en el plan director para el año 2025. Ver Figura 32 “Valoración efectividad de controles”.

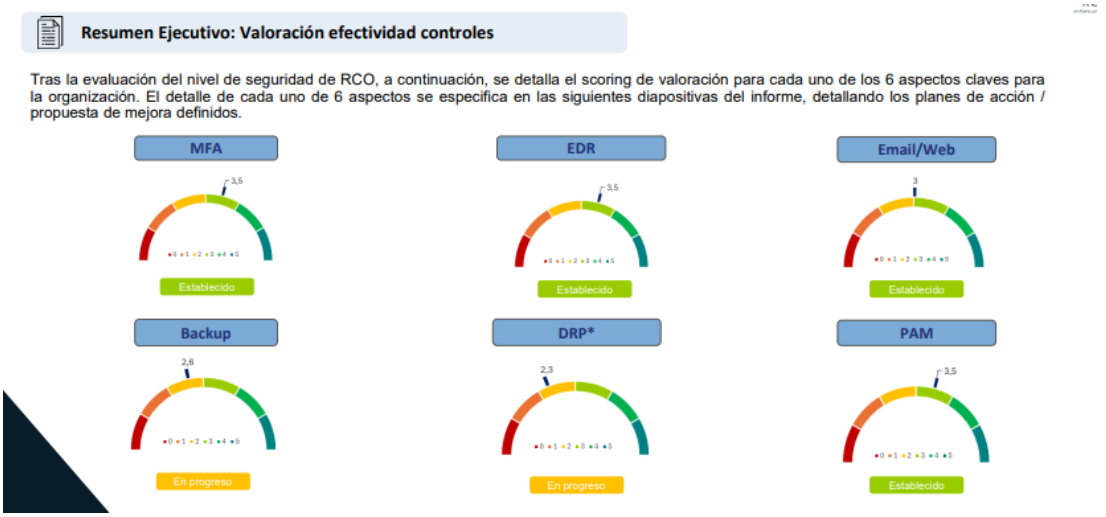


Figura 32 “Valoración efectividad de controles”

7. Pruebas de penetración

Ultimo pen test realizado septiembre 2024:

En la figura 33, titulada "Vulnerabilidades Detectadas", se presenta el detalle de las vulnerabilidades identificadas durante este escaneo, y en la figura 34 “Vulnerabilidades por severidad”. Las vulnerabilidades de alto impacto serán abordadas durante el mes de noviembre de 2024. Para diciembre de 2024, se espera que todas las vulnerabilidades detectadas hayan sido completamente resueltas.

RCO
an Abertis company

6 Vulnerabilidades identificadas

Durante las pruebas de penetración se identificaron un total de 11 vulnerabilidades únicas que deberán ser atendidas de acuerdo con la siguiente referencia:

Severidad	Vulnerabilidades únicas	Incidencias	Tiempo de atención
Crítica	0	0	Inmediatamente
Alta	4	189	Corto plazo
Media	5	413	Mediano plazo
Baja	2	107	Largo plazo

Tabla 4. Vulnerabilidades por incidencia

Figura 33 “Vulnerabilidades detectadas”

A continuación, se muestra la gráfica de los impactos identificados con el respectivo número de incidencia y severidad:

Gráfico 1. Vulnerabilidades únicas identificadas por severidad

Figura 34 “Vulnerabilidades por severidad”

8. Plan de respuesta a incidentes.

Un plan de respuesta a incidentes hubiera marcado una gran diferencia en el momento del incidente ya que, se actuó de manera correcta, pero pudo ser menos doloroso si cada uno de los involucrados hubiera tenido de manera previa que papel debía jugar y cuál era su aportación en el incidente. Por lo que se creó un proceso de respuesta a incidentes, en el cual nuestro proveedor Minsait que es nuestra oficina virtual de seguridad juega un papel importante.

El propósito de este documento es establecer una estructura operativa, así como los procesos y procedimientos para la gestión de incidentes de seguridad de Red de Carreteras de Occidente (en adelante, RCO). Se definen las actividades que deberán llevar a cabo los grupos de atención para preparar, detectar, analizar, contener, erradicar, recuperar y aplicar las lecciones aprendidas, todo ello en el menor tiempo posible, con el objetivo de minimizar el impacto en la organización.

El alcance de este documento es establecer en RCO un marco integral de procesos y procedimientos para identificar, gestionar, investigar y remediar una amplia gama de incidentes de seguridad de la información. Proporciona una guía clara para activar una respuesta efectiva y establece la estructura necesaria para asegurar la ejecución coordinada de las acciones requeridas ante un incidente. Además, hace referencia a la documentación procedimental que detalla las actividades operativas específicas para manejar ciertos tipos de incidentes (*Playbooks).*

Dado que no es posible anticipar o prever todos los escenarios posibles, este documento debe integrarse con el manual de crisis y los planes de recuperación ante desastres (DRP) y continuidad del negocio (BCP). Esto garantiza que la alta dirección y los equipos involucrados cuenten con información clave para la toma de decisiones, permitiendo una visión holística y global en la gestión de crisis.

Para el desarrollo y mantenimiento de este plan, se han utilizado los siguientes documentos y normas de referencia:

- *Scottish Goverment: Cyber Capability Toolkit*
- NIST SP 800-61: "*Computer Security Incident Handling Guide*"
- ISO/IEC 27035: "*Information security incident management*"
- ISO/IEC 27001: "*Information Security Management Systems*"
- ISO/IEC 27002: "*Code of practice for information security controls*"
- Política de Seguridad de la Información de RCO

Este plan está destinado a:

- Miembros del equipo de respuesta a incidentes (IRT)
- Personal operativo de TI
- Jefaturas y coordinaciones de TI

- Dirección de TI
- Empleados y proveedores que interactúan con los sistemas de información de la organización

Los objetivos principales de la respuesta a incidentes son:

- Detección y Notificación Rápida: Identificar y reportar incidentes de seguridad de manera oportuna para minimizar el impacto.
- Contención y Erradicación Eficaz: Limitar la propagación del incidente y eliminar la causa raíz de manera eficiente.
- Recuperación y Restauración: Recuperar los sistemas afectados y restaurar las operaciones normales lo más rápido posible.
- Minimización del Impacto: Reducir el impacto negativo en las operaciones de la organización, la reputación y la confianza de los clientes.
- Lecciones Aprendidas: Analizar los incidentes para identificar lecciones aprendidas y mejorar continuamente los procesos y controles de seguridad.

Metodología de tratamiento de respuesta a incidentes

La metodología de respuesta a incidentes en RCO es un enfoque híbrido que combina elementos del marco NIST 800-61 R2 y la norma ISO 27035. Este modelo se estructura en seis fases interconectadas y cíclicas: preparación, detección, análisis, contención, erradicación y recuperación, y lecciones aprendidas, Figura x “Fases de respuesta a incidentes”. Estas fases proporcionan una estructura organizada y resolutiva, permitiendo a RCO prepararse y responder de manera eficaz ante incidentes de seguridad, minimizando el impacto potencial en la organización.

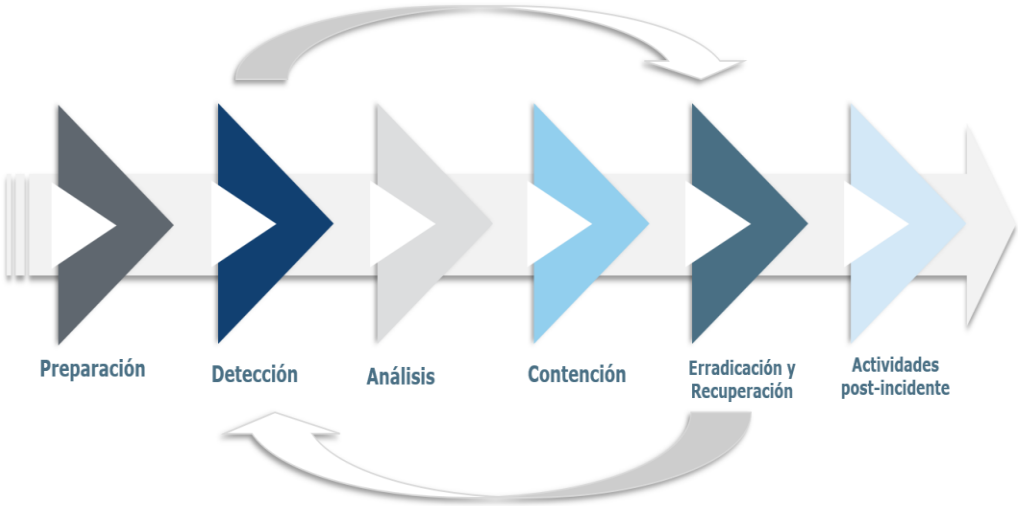


Figura 35 “Fases de respuesta a incidentes”

En la siguiente tabla 2 “objetivos”, se muestran los principales objetivos de cada fase.

Fases del modelo	Objetivos
Preparación	• Fortalecer la capacidad de resiliencia ante incidentes de seguridad. • Desarrollar la documentación necesaria que establezca el proceso a seguir durante un incidente. • Definir y comunicar los roles y responsabilidades de los equipos encargados de la respuesta ante incidentes.
Detección	• Identificar y notificar cualquier violación o compromiso de la confidencialidad, integridad o disponibilidad de los datos de la organización.
Análisis	• Realizar una investigación preliminar del incidente de seguridad. • Notificar al personal adecuado sobre el ataque o la información comprometida. • Determinar la necesidad de una investigación forense completa. • Elaborar un plan de remediación basado en el alcance y las características del incidente.
Contención	• Contener y mitigar los efectos del incidente de seguridad en los sistemas afectados. • Evaluar si es necesario realizar un análisis forense adicional para obtener más detalles sobre el incidente.
Erradicación Y Recuperación	• Eliminar completamente la amenaza o vulnerabilidad de los sistemas y redes afectadas, aplicando las medidas de mitigación necesarias. • Restaurar los sistemas, servicios y operaciones afectados a su estado normal, garantizando que estén completamente funcionales y libres de cualquier compromiso de seguridad.
Lecciones aprendidas	• Elaborar un informe detallado del incidente, que incluya todas las actividades realizadas. • Completar la revisión de lecciones aprendidas y gestionar las mejoras identificadas para prevenir futuros problemas.

Tabla 2 “objetivos”

La priorización la podemos observar en la tabla 3 “Matriz de prioridad de incidentes”, de atención es definida por las siguientes categorías, lo podemos observar en la tabla 4 “Nivel de urgencia de incidentes” de acuerdo con que tan apremiante es el incidente de seguridad:

Matriz de prioridad de Incidentes		Impacto funcional		
		H	M	L
Impacto en la información	H	5	4	3
	M	4	3	2
	L	3	2	1

Tabla 3 “Matriz de prioridad de incidentes”

Nivel de urgencia	Descripción
5	Crítico
4	Alto
3	Medio
2	Bajo
1	Muy bajo

Nivel de urgencia del incidente

Durante un incidente de seguridad, RCO deberá recopilar los datos clave generados, relacionados con el evento adverso, con el fin de obtener una mayor contextualización y proporcionar información detallada sobre la detección del incidente. Para facilitar este proceso, se han implementado las siguientes herramientas de apoyo provistas por el Equipo Externo de Respuesta a Incidentes (Minsait):

Registro de comunicación: Este documento tiene como objetivo centralizar toda la información relativa a las comunicaciones establecidas durante el ciclo de vida de un incidente de seguridad. Se registrarán detalles como la fecha, hora, método de comunicación, personas involucradas y el contenido de cada intercambio. El personal de ciberseguridad de RCO será responsable de mantener este registro hasta que el Equipo Externo de Respuesta a Incidentes (Minsait) intervenga.

Pesquisa del incidente: Este documento está diseñado para capturar información relevante sobre la detección del incidente y contribuir a la investigación. Se incluirán datos como el detalle de los servicios, sistemas y/o aplicaciones afectadas, el número de entidades impactadas, y la naturaleza del incidente. El personal de ciberseguridad de RCO será responsable de esta recopilación hasta que el Equipo Externo de Respuesta a Incidentes (Minsait) intervenga.

En la figura 36 “Proceso de incidentes” podemos observar de manera detallada quienes son los involucrados y como fluye el proceso entre todas las áreas.

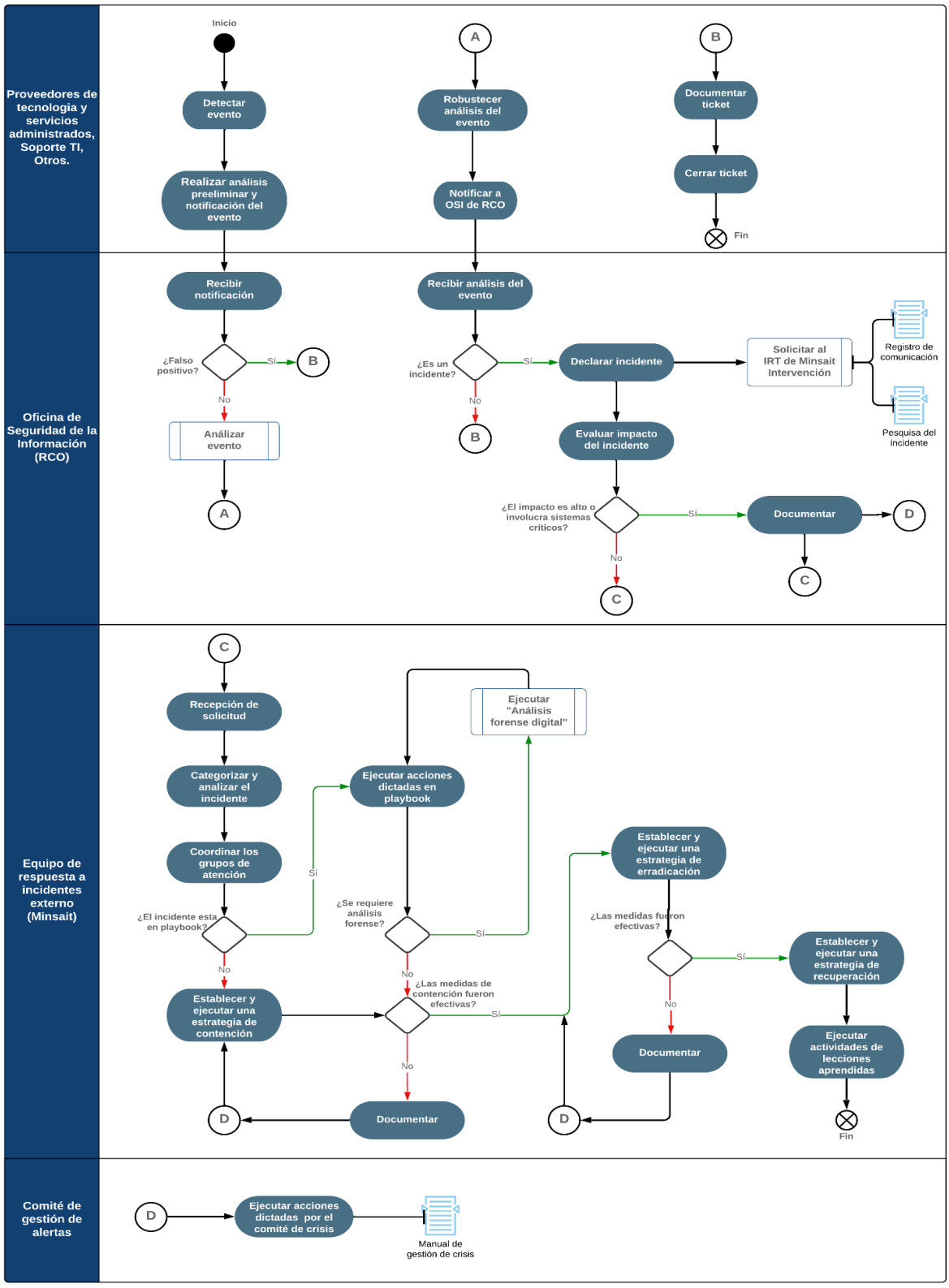


Figura 36 “Proceso de incidentes”

9. La manera más fácil de vulnerar la seguridad de una red corporativa es mediante un usuario.

Contar con un equipo de trabajo adecuadamente capacitado y consciente de las mejores prácticas en seguridad de la información y ciberseguridad es clave para agilizar las acciones de respuesta. En el caso de RCO, la falta de un equipo con la capacitación adecuada llevó a errores en la gestión y respuesta del incidente, ya que el personal no estaba familiarizado con los protocolos o planes a seguir. Se implemento un programada calendarizado de comunicación en temas de seguridad de la información. En la figura 37 “Ejemplo de Plan de comunicación” se envían a toda la organización *tips* de seguridad o bien actividades necesarias para actualizaciones de los equipos.

Figura 37 “Ejemplo de Plan de comunicación”

RCO tiene contratada una oficina de seguridad, su función es ser un equipo extendido de ciberseguridad en donde nos mantienen permanentemente actualizados en temas de seguridad de la información, en la figura 38 “Alerta de amenaza” tenemos un ejemplo de una amenaza que se detectó de manera reciente en este caso de Microsoft.

minsait

An Indra company

ALERTA DE AMENAZA

FECHA:25/10/2024 **SEVERIDAD: ALTA**

Actores de amenazas despliegan el loader Latrodectus buscando comprometer a usuarios de sistemas Windows

IDENTIFICADOR	SECTOR	ACTOR DE AMENAZA
Latrodectus	Multiples	TA577 y TA578
OBJETIVO	**TIPO**	**VECTOR DE ATAQUE**
Despliegue de malware adicional	Loader	Phishing

DESCRIPCIÓN

Investigaciones han identificado campañas phishing que buscan distribuir el loader Latrodectus, también conocido como Black Widow, IceNova o Lotus, por parte de actores de amenazas como TA577 y TA578, en las campañas se ha observado que intenta suplantar entidades como Microsoft Azure y Cloudflare. No obstante, en la más reciente, se hacen pasar por el software de firma electrónica DocuSign en donde invitan a la víctima acceder al enlace fraudulento para poder descargar el supuesto documento, que es un archivo JavaScript altamente ofuscado y de gran tamaño que tiene como objetivo descargar y ejecutar un archivo MSI que utiliza rundll32.exe para cargar una DLL modificada, este se inyecta en el proceso explorer.exe y carga una DLL falsa de con el nombre de Nvidia para ocultar sus actividades maliciosas, y así comunicarse con servidores de comando y control mediante el puerto 8041 y descargar malware adicional

CAPACIDADES

- Robo de información.
- Ofuscación de código
- Ejecución de código.
- Evasión de herramientas de seguridad.
- Despliegue de malware adicional.
- Comunicación con servidores de comando y control (C2).

RECOMENDACIONES

Latrodectus es un loader altamente especializado que se distribuye mediante campañas phishing que buscan engañar a los usuarios para descargar y ejecutar archivos maliciosos, por lo que se recomienda ampliamente:

- Bloquear los indicadores de compromiso (IoCs) compartidos.
- Evitar el uso de equipos corporativos para realizar trámites o pagos personales.
- Verificar que las tecnologías cuenten con las últimas actualizaciones instaladas.
- Mantener en monitoreo las comunicaciones por el puerto 8041.
- Realizar campañas de concientización al personal sobre tácticas de ingeniería social y phishing.
- Verificar la autenticidad de los mensajes recibidos y evitar compartir información personal.

CADENA DE COMPROMISO DEL LOADER LATRODECTUS

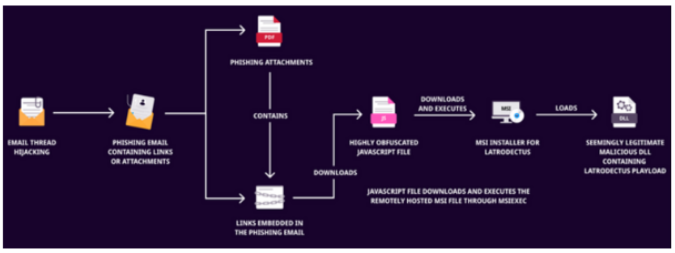


Figura 38 “Alerta de amenaza”

10. Análisis de impacto al negocio (BIA)

Este análisis fue realizado por un proveedor NTT Data, en marzo de 2024, ya habíamos tenido el incidente.

El BIA es la base fundamental para implementar un programa de gestión de la continuidad del negocio, en él se determinan los impactos generados ante la materialización de riesgos que puedan afectar la operación de los procesos y así mismo la disponibilidad de los servicios que entrega la organización a sus clientes. Con base en el análisis de esos impactos se pueden determinar los procesos críticos y definir los Tiempos Objetivo de Recuperación (RTO) y los Puntos Objetivo de Recuperación (RPO) o Tiempo máximo permisible de pérdida de datos, y de esta manera priorizar procesos y recursos que es el insumo y así en una etapa posterior, definir estrategias de continuidad de negocio, que permitan minimizar los impactos generados ante la ocurrencia de desastres en la organización.

El desarrollo del BIA de RCO, se ha realizado bajo la metodología de ISO 22317:2015, teniendo en cuenta igualmente las buenas prácticas de continuidad de negocio del BCI (Business Continuity Institute) y alineado con lo establecido en el estándar de Sistemas de Gestión de Continuidad de Negocio (ISO 22301).

Objetivo:

- Identificación de los procesos críticos: Identificar los impactos cualitativos y cuantitativos, resultantes de detener la operación de los procesos críticos.
- Identificar el tiempo máximo tolerable de indisponibilidad del proceso (MTPD, por sus siglas en inglés).
- Identificar la criticidad de los procesos en función de los impactos: reputacional, servicio al cliente, regulatorio, financiero (gasto e ingreso), relación con colaboradores, y relación con proveedores de RCO, las necesidades externas e internas y el impacto económico que la no ejecución/interrupción de dichos procesos pudiera provocar.
- Obtener del Tiempo de Recuperación Objetivo (RTO) para cada proceso.
- Delimitar el Punto de Recuperación Objetivo (RPO) al que la información tiene que ser restaurada para que un proceso opere una vez se ha reiniciado.

En consecuencia, los objetivos del BIA son: Identificar los periodos de tiempo más vulnerables para la operación.

- Identificar los mecanismos alternos de operación en caso de no contar con información, aplicaciones, instalaciones o colaboradores.
- Identificar los eventos de interrupción de mayor frecuencia.

- Identificar y especificar las interdependencias de los subprocesos.
- Identificar los recursos mínimos (personal, mobiliario y equipos, entre otros) importantes para la operación.

ALCANCE

El alcance del BIA está enmarcado para los procesos *core* de negocio de RCO que se relacionan a continuación, los cuales fueron validados previamente por RCO para el desarrollo del BIA:

- Servicios Auxiliares
- Peaje
- Gestión Vial
- Facturación

ENFOQUE Y METODOLOGÍA

Evaluación de la madurez

Siguiendo las mejores prácticas definidas por el Disaster Recovery Institute (DRI) y lo dispuesto por la Organización Internacional de Normalización (ISO) en la norma ISO/TS 22317:2015. Se han definido una serie de pasos o fases para llevar a cabo la evaluación de impacto al negocio, mismos que son detallados a continuación.

Fase 1: Definición de criterios de evaluación.

Se llevó a cabo la determinación de grupos de interés, asignación de porcentajes y tabla de impactos de referencia, como lo podemos observar en la figura 39 “Grupos de interés”

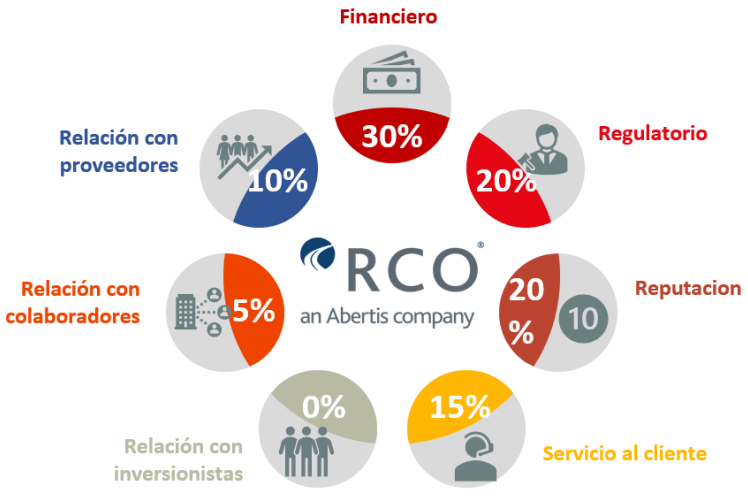


figura 39 “Grupos de interés”

Fase 2: Selección de procesos.

Se realizó una selección de procesos/actividades core del negocio de RCO, dichos procesos/actividades fueron listados previamente en el alcance.

Fase 3: Identificación de procesos críticos.

Se realizó la identificación de impactos cualitativos y cuantitativos, del Máximo Tiempo Tolerable de Interrupción (MTPD, por sus siglas en inglés) y de la criticidad relativa de los procesos. Ver figura 40 “Niveles de impacto”

Nivel de Impacto	Reputación	Servicio al cliente	Regulatorio	Impacto Financiero (Gasto e Ingreso)	Relación con colaboradores	Relación con proveedores
5 Extremo	• Posible pérdida desconfianza dentro del medio. (Ej: desconfianza de clientes, inversionistas, proveedores por vialidad del negocio) • Afectación de la percepción de los inversionistas, proveedores y clientes.	• Interrupción prolongada del servicio, percibida por varios clientes.	• Posibilidad de ser acreedor al pago de multas, penalizaciones o sanciones. • Incumplimiento significativo en normas o regulaciones fiscales, federales, estatales, de comercio exterior o regulaciones financieras. (CNBV, CONDUSEF, BM, SAT, STPS, IMSS, Infonavit, etc.)	• Se incurre en un incremento del gasto no previsto. • Se incurre en pérdidas financieras que afectan el ingreso de la empresa. • Afecta parcialmente la percepción de ingresos. • Mas de 40 millones de euros	• Posible descontento generalizado.	• Se comienza a afectar la relación con el proveedor. • Incumplimiento de compromisos contractuales, con posibilidad de aplicación de sanciones. • Número significativo de proveedores afectados.
4 Relevante	• Posible afectación de la percepción de los inversionistas, proveedores y clientes. (Ej: Inconformidad de proveedores con impacto en relación comercial).	• Interrupción temporal del servicio, percibida por más de 1 cliente.	• Incumplimiento parcial en normas o regulaciones fiscales, federales, estatales, de comercio exterior o regulaciones financieras. (CNBV, CONDUSEF, BM, SAT, STPS, IMSS) • Incumplimiento total de políticas / reglamentos internos.	• Se incurre en un incremento del gasto no previsto. • Se incurre en pérdidas financieras. • Se genera una disminución en los ingresos. • Entre 25 y 40 millones de euros	• Descontento en varias áreas. • Pérdida de confianza.	• No se afecta la relación con el proveedor. • Algunos proveedores afectados.
3 Significativo	• Criticas dentro del medio. (Ej: Competidores, proveedores o clientes).	• Interrupción temporal de servicio, que tiene la posibilidad de ser percibida por al menos 1 cliente.	• Posible incumplimiento en normas o regulaciones fiscales, federales, estatales, de comercio exterior o regulaciones financieras. (CNBV, CONDUSEF, BM, SAT, STPS, IMSS, Infonavit, etc.) • Incumplimiento significativo de políticas / reglamentos internos.	• Se comienzan a generar gastos no previstos. • Perdidas no recuperables (Ej: nuevos clientes.) • Se comienzan a presentar pérdidas financieras menores. • Entre 15 y 25 millones de euros	• Personal insatisfecho en una o dos áreas. • Poca pérdida de confianza.	• Algunos proveedores conscientes del problema, es la pérdida temporal y/o mínima de operación.
2 Limitado	• Posible disminución de la confianza dentro de la organización.	• Breve interrupción del servicio, que tiene la posibilidad de ser percibida por al menos 1 cliente.	• Incumplimiento parcial de políticas / reglamentos internos.	• Posibilidad de generar gastos no previstos • Posibilidad de dejar de percibir ingresos previstos. • Demora la percepción de ingresos, pero es recuperable. • Entre 5 y 15 millones de euros	• Al menos 1 área consiente del problema. • Posible pérdida de confianza.	• Los proveedores no son afectados o no perciben el problema. • Impacto irrelevante.
1 Insignificante	• Sin impacto reputacional.	• Breve interrupción del servicio, que no es percibido por los clientes.	• Posible incumplimiento de políticas / reglamentos internos.	• Perdidas menores a 5 millones de euros.	• Posibles molestias en el personal. • No hay pérdida de la confianza.	• Sin impacto.

Ver figura 40 “Niveles de impacto”

Fase 4: Análisis de procesos críticos.

Se realizó el levantamiento de información a través de cuestionarios aplicados a los dueños de los procesos. La información obtenida para el análisis de impacto al negocio fue: **Identificación de dependencias:**	¿Cuáles son los Insumos/Entradas (Áreas, entidades) que entregan información para iniciar la ejecución del proceso?
	¿Cuáles son los proveedores críticos que se requieren para la ejecución del proceso?
Identificación de Requerimientos Tecnológicos:	¿Cuáles son los aplicativos requeridos y la criticidad considerada?,
	¿Cuál es el tiempo de tolerancia a la actualización de los datos?,
	¿Cuál es el tiempo de tolerancia de recuperación del aplicativo?
Identificación de Periodos Críticos:	¿Cuál es la frecuencia con la que se realiza el proceso (Eventual, diaria, semanal, quincenal, mensual, anual)?
	¿Cuáles son las semanas y meses más críticos?

RESULTADOS

Se evaluaron 4 procesos como parte del alcance del BIA. En los cuestionarios aplicados a los dueños de los procesos se les solicitó identificar los impactos que tendrían sus procesos en caso de detenerse en distintos periodos de tiempo (4 horas, 8 horas, 2 días, 1 semana y más de 1 semana), para realizar dicha evaluación se basaron en la tabla de impactos definida.

Posteriormente, los resultados obtenidos se ponderaron con los porcentajes establecidos a los distintos grupos de interés. Del análisis anterior se obtuvo un criterio de evaluación que se denominó “Criticidad residual”.

En las siguientes secciones del presente documento, se presentan los resultados finales obtenidos a partir del análisis aplicado a la información de los procesos. Estos resultados se muestran en forma de tablas y gráficos, con sus respectivas explicaciones, con la finalidad de simplificar los resultados y las principales conclusiones. La valoración final de cada rango de tiempo se calcula con base a la criticidad asignada por el entrevistado (1 al 5) y los porcentajes asignados a cada grupo de interés, la valoración final está en un rango de 0 al 100%.

EVALUACIÓN DE IMPACTOS POR PROCESO

La siguiente figura 41 “Nivel de impacto”, presentan la valoración del impacto residual del proceso, la cual se deriva de los niveles de impacto que el dueño del proceso asignó y la ponderación de estos, usando los criterios de evaluación definidos previamente en la ruleta de impactos.

IMPACTOS	< 4 HORAS	4 - 8 HORAS	1 -3 DÍAS	1 SEMANA	> 1 SEMANA
Reputación	2	2	4	5	5
Servicio al cliente	3	4	5	5	5
Regulatorio	4	5	5	5	5
Financiero	1	1	1	1	1
Relación con colaboradores	3	4	4	5	5
Relación con proveedores	4	5	5	5	5

Figura 41” Nivel de impacto”

Del análisis se puede resaltar lo siguiente:

A una semana sin operación surgen afectaciones en los acuerdos contractuales con las franquicias.

- Incumplimiento en los títulos de concesión.
- Incumplimiento para generar facturas, lo que ocasiona posibles problemas en caso de empezar a recibir denuncias por parte de los clientes.
- Existe una pérdida de reputación con las franquicias y clientes.

La siguiente figura 42 “Indicadores de recuperación” muestra la prioridad de recuperación, basada en los tiempos máximos tolerables de interrupción, sin embargo, esta priorización puede variar dependiendo de la particularidad del escenario que se presente, por ejemplo: se puede dar prioridad a los procesos que no cuentan con mecanismos alternos de trabajo, o los procesos con restricción de horario para operar. En otras palabras, esta es una opción de priorización que deberá ser evaluada de acuerdo con el tipo y a la afectación de la contingencia que se presente, así como al horario y día de que se trate.

MTPD	RTO	RPO
2 semanas	1 semana	1hora

Figura 42 “Indicadores de recuperación”

El proceso evaluado proporcionó aplicaciones vitales para su operación, las cuales se les asignó una criticidad y un tiempo de recuperación objetivos, dicha información se muestra a continuación:

Principales Herramientas de trabajo (software)

Aplicación	Criticidad	RTO (hrs)
Software de punto de venta	Alto	84
Internet	Alto	84
Bitácoras de Apex	Alto	84
Portal de proveedores	Medio	168
Reportes Operativos (Idral)	Medio	168
Correo electrónico	Medio	168
Base de datos	Medio	168
Office 365	Medio	168

Personal

Identificar el total del personal que está a cargo de los procesos en funcionamiento normal y cuántos serían los mínimos necesarios por considerar en caso de una contingencia, lo cual permite determinar el grado de dependencia que tienen los procesos críticos con respecto a los aplicativos, información, instalaciones y colaboradores. Ver figura 43 “Personal”

Personal actual	Personal mínimo para continuar con las operaciones	Proceso alterno
61	50	Si

Ver figura 43 “Personal”

Del análisis se puede resaltar lo siguiente:

1. El proceso tiene una alta dependencia del personal que lo opera normalmente.

2. El proceso tiene una dependencia de los aplicativos tecnológicos que se ocupan para su operación.

3. El proceso tiene dependencia de la información, ya que no pueden ser ejecutados si no tienen acceso a ella.

4. Gestión Vial cuenta con un proceso alterno, el cual se puede ejecutar para llevar la operación, el cual es el “Plan de continuidad de la operación”.

5. El plan de continuidad de la operación cuenta con diferentes riesgos identificados y planes alternos de operación, sin embargo, no contempla aspectos técnicos que componen

el proceso, por lo que es importante contar con los activos relacionados con el proceso debidamente identificados para generar estrategias de recuperación ante desastres.

Interdependencias: Las entradas de los procesos críticos son consideradas críticas, ya que son indispensables para la ejecución de los procesos, de ahí la importancia de identificarlas y analizarlas. En la siguiente tabla se identifican aquellas entradas (áreas, aplicaciones, procesos, etc.). Se detallan en las figuras 44 “áreas”, figuras 45 áreas“

Nombre del proceso	Fuente (Proceso de negocio)	Entrada (Doc. o información)	Tratamiento (Actividad (El realizado dentro del proceso evaluado))	Producto o resultado (Doc. o información)	Destino (Proceso de negocio o proveedor externo)
Servicios Auxiliares	Facturación	PDF y XML Cuentas correo estándar	Facturación de compras por diferentes proveedores Evalúan los números de cada marca y unidad de negocio	El encargado reporta a líderes de marca	Compras Venta
Servicios Auxiliares	Ventas	Notas de venta se envía de modo manual	Sacan la información de los puntos de ventas y ven que todo sea dueños del proceso	Reporta directo a dirección de operaciones	Dirección de operaciones.
Servicios Auxiliares	Compras	Montos de los ingresos. Este es automatizado vía correo electrónico	El proveedor envía la información a una cuenta de correo estándar.	Informes de los ingresos.	Líder de marca
Servicios Auxiliares	Tiendas y franquicias	Lista de precios Documentación de inventarios	Se reportan los costos correspondientes a cada periodo, los valores de los inventarios	Documentos de reportes	Contabilidad
Servicios Auxiliares	Colaborador	Cartas de vacaciones laborales	Interacciones para altas y bajas Incapacidades Reporte de vacaciones Toda relación con lo que se requiere para los colaboradores.	Cartas de vacaciones laborales	Persona y organización RH
Servicios Auxiliares	Colaborador	Aviso de accidente de trabajo (incapacidad)	Reportes de los incidentes de trabajo	Documentos de reportes	Gerencia de seguridad de higiene Servicios

Figuras 44 “áreas”

Nombre del proceso	Fuente (Proceso de negocio)	Entrada (Doc. o información)	Tratamiento (Actividad (El realizado dentro del proceso evaluado))	Producto o resultado (Doc. o información)	Destino (Proceso de negocio o proveedor externo)
Servicios Auxiliares	Tiendas y franquicias	Información financiera	Planeación y control para todo el seguimiento de presupuestos	Documentos de reportes	Finanzas
Gestión Vial	Llamadas de emergencia	Registros que se realizan	Información que llega al centro de control Llamadas que son generadas por los usuarios	Informes Se genera reporte de título concesión a secretaria	Secretaria
Gestión Vial	Llamadas de emergencia	Registros que se realizan	Información que llega al centro de control Llamadas que son generadas por los usuarios	Informes a dirección los indicadores KPI's	Dirección
Peaje	Caseta de cobro vial	Envió de informes de los colaboradores (cobrador) Telepeaje	Se realiza una validación en cada corte de turno(pre liquidación), verifican lo que entrega en cobrador con lo que está en el sistema	Informes de tráfico de red Informes de auditoría interna	Secretaria
Peaje	Caseta de cobro	Envió de informes de los colaboradores (cobrador) Telepeaje Caseta de cobro (Tarjeta/Efectivo) Tag	Se realiza una validación en cada corte de turno(pre liquidación), verifican lo que entrega en cobrador con lo que está en el sistema	Informes de tráfico de red Informes de auditoría interna	Auditoría interna de peaje
Peaje	Caseta de cobro	Registros de facturación en sitio	Se realizan Facturación en los sitios, en caso de que los usuarios lo soliciten.	Reportes de facturación	Facturación
Facturación	Autoridad fiscal	Documentos e informes de entradas financieras Se descarga la información	Presentan una serie de declaraciones mensuales Informes a la comisión nacional bancaria Estados financieros Información	Declaraciones e Informes	Comisión Nacional Bancaria

Figura 45 “Áreas”

Nombre del proceso	Fuente (Proceso de negocio)	Entrada (Doc. o información)	Tratamiento (Actividad (El realizado dentro del proceso evaluado))	Producto o resultado (Doc. o información)	Destino (Proceso de negocio o proveedor externo)
			contable y financiera		
Facturación	Control de gestión	Documentos e informes de entradas financieras Formatos	Se hace un reporte interno, se realizan formatos que se presentan mes a mes, semestral o anualmente	Reporte corporativo	Área control de gestión
Facturación	Control de gestión	Información de impuestos	Realizan presentaciones del control de impuestos	Presentaciones	Control de gestión
Facturación	Compras	Documentos e informes de entradas financieras	Servicio de asesoría fiscal Se envían cuestionamientos para asesorar si es apto el proveedor, aplica especialmente para proveedores extranjeros. Revisión de contratos, residencias fiscales.	Reenvía el cuestionario con las anotaciones, si es apto.	Compras
Facturación	Cuentas por pagar	Pagos al extranjero	Se revisa si tiene alguna retención, se da las pautas, y feedback	Documentos autorizados para efectuar el pago.	Cuentas por pagar
Facturación	Legal	Temas de contratos y licitaciones Conexión con el equipo AP	Revisan contratos desde una óptica fiscal que cumplan con todos los requerimientos, se puede dar el Visto bueno o se da una serie de cláusulas que se deben ser tomadas en cuenta.	Contratos con las modificaciones y observaciones	Legal

Figura 46 “Áreas”

Del análisis se puede resaltar lo siguiente:

- Servicios Auxiliares en términos fiscales es el área más robusta, pero no se cuenta con un control óptimo y no está bien establecido a nivel fiscal.
- Peaje no tiene un proceso estructurado en temas de factura global.
- Facturación tiene relación con la mayoría de las áreas de RCO, menos con las áreas operativas.
- El área de Atención al cliente tiene consultas de problemas en facturación.
- Facturación tiene relación directa con el corporativo de Abertis, con el área fiscal. Se da un feedback sobre las auditorías, se realiza un reporte en específico, puede ser trimestral, semestral o anual.

Conclusiones:

De acuerdo con el resultado del análisis realizado podemos concluir lo siguiente:

- A partir de 3 días de interrupción, los impactos para RCO empiezan a ser relevantes, por lo que los planes de recuperación deben estar orientados a restablecer las operaciones normales en no más de 12 horas en promedio.
- El proceso de facturación después de analizar las respuestas del responsable y considerando que es uno de los principales procesos para las actividades financieras de RCO, los tiempos de recuperación para este proceso deben ser prioridad con un objetivo de recuperación no mayor a 3 días.
- Los procesos de peaje y gestión vial tienen relevancia para la organización y los impactos de no contar con estos procesos son significativos. tanto para los clientes como para los procesos internos, se observan impactos significativos a partir de una semana de interrupción.
- Hay que considerar que estos procesos tienen planes alternativos de trabajo en caso de algún tipo de interrupción, por lo que se recomienda tener como objetivo de recuperación de actividades un periodo de recuperación no mayor a 12 horas.
- La 3.ª y 4.ª semana del mes son las de mayor operatividad promedio de los procesos críticos, por lo que estas semanas deberán ser consideradas como las más relevantes para la operación de RCO y en consecuencia deben ser consideradas como máxima prioridad en los planes de recuperación.
- La mayoría de los procesos críticos no cuentan con recursos alternos en caso de indisponibilidad de información y aplicativos, por lo que la creación de estrategias de recuperación será vital para atender esta dependencia, con el fin de disminuir el tiempo de inactividad de las aplicaciones críticas.
- Contar con un sistema efectivo de respaldos ayudaría a reducir los tiempos de inactividad por perdida de información.
- Existe alta dependencia de la información, por lo cual tener planes de comunicación y copias de seguridad programadas y ejecutadas es fundamental para la continuidad de las operaciones.
- Los criterios que se determinaron en las sesiones deberán ser evaluados de acuerdo con el tipo de contingencia de que se trate, al momento en que se presente y al tipo de afectación que tenga, por ejemplo: se puede dar prioridad a ciertos procesos críticos, o a los procesos que no cuentan con mecanismos alternos de trabajo, o los procesos con restricción de horario para operar, etc.
- Esta información será insumo para la creación de estrategias y la determinación de criterios de toma de decisión.

- Los servidores principales donde se almacena la información son en los NAS, existen respaldos. Los servidores deben considerarse activo, crítico, ya que los 4 procesos son dependientes de la información, para continuar con sus actividades.

- Los procesos de peaje y gestión vial tienen una alta dependencia de Indra, por lo que es importante contar con los acuerdos necesarios con este proveedor para asegurar el correcto funcionamiento de los servicios proveídos y asegurar que existen los correctos controles de seguridad implementados en sus sistemas para reducir la posible explotación de debilidades.
- Mantener los registros actualizados, sobre los cambios en la estructura organizacional en toda la cadena de información de RCO.
- Llevar a cabo capacitaciones periódicas y realizar una campaña muy fuerte de difusión sobre la importancia de la Continuidad de Negocio y de la seguridad de la información y el papel medular que todos en RCO jugamos, para evitar:

- Una evaluación incorrecta de los impactos.
- No estimación de los impactos financieros.
- Falta de justificación de la información proporcionada.
- Evaluaciones poco objetivas.
- Que los datos proporcionados no sean completos.

- Es importante asegurar que las personas alternas a ocupar cargos durante una contingencia sean debidamente capacitadas para asegurar la correcta ejecución de las actividades/procesos.
- Iniciar con la gestión documental de los procedimientos operativo alterno, para ejecutar actividades de manera temporal cuando el procedimiento original no se puede llevar a cabo debido a una contingencia.
- Implementar un sistema de gestión de riesgos con terceros para asegurar la continuidad de prestación de servicios.
- Debido a la alta dependencia con las aplicaciones es importante que estas y los servidores que las soportan cuenten con sus debidos planes de continuidad de servicio para asegurar la disponibilidad ante diferentes incidentes.
- Se recomienda llevar a cabo un análisis de riesgos para identificar otros procesos dentro de RCO que pudieran ser importantes para las estrategias de recuperación y continuidad de negocio.

- Servicios Auxiliares en términos fiscales es el área más robusta, se recomienda implementar un control óptimo, seguro y bien establecido a nivel fiscal.
- Gestionar e implementar un proceso estructurado en temas de factura global, para la gestión del proceso de peaje.
- Disponer de personal suficientemente capacitado y especializado, capaz de enfrentarse a los eventos inesperados que atentan con la operatividad, seguridad y disponibilidad de los sistemas de información y las comunicaciones.

Bibliografía

1. Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Zero-day aware decision fusion-based model for crypto-ransomware early detection. *Computers & Security*, 74, 160-174. https://doi.org/10.1016/j.cose.2017.10.010
2. Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). *Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions*. *Computers & Security*, 74, 144-166.
3. Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Zero-day aware decision fusion-based model for crypto-ransomware early detection. *Computers & Security*, 74, 160-174
4. Business Continuity Institute. (2024). *Business continuity planning.* Recuperado de https://www.thebci.org/bcp
5. Cobb, M. (2023). *Incident response plan essentials: How to prepare for a data breach*. SearchSecurity. Recuperado de https://www.techtarget.com/searchsecurity
6. Cole, E. (2012). *Advanced persistent threat: Understanding the danger and how to protect your organization*. Syngress.
7. Cybersecurity & Infrastructure Security Agency (CISA). (2024). *Las principales técnicas de prevención contra ataques de ransomware*. CISA. https://www.cisa.gov/stopransomware/how-can-i-protect-against-ransomware
8. Europol. (2022). *The Internet Organized Crime Threat Assessment (IOCTA)*. Europol. https://www.europol.europa.eu/media-press/newsroom/news/crime-in-age-of-technology-%E2%80%93-europol%E2%80%99s-serious-and-organised-crime-threat-assessment-2017
9. ENISA, The European Union Agency for Cybersecurity. (2023). *Ransomware: Trends, techniques, and threats*. ENISA. https://www.enisa.europa.eu/publications/ransomware-trends-techniques-and-threats
10. Gartner, Inc. (2024) Business Continuity Planning (BCP). Recuperado de https://www.gartner.com/en/newsroom
11. International Organization for Standardization. (2019). *ISO 22301:2019 - Societal security – Business continuity management systems – Requirements*. ISO. Recuperado de https://www.iso.org/standard/
12. Kharraz, A., Arshad, S., Mulliner, C., Robertson, W. K., & Kirda, E. (2016). *Cutting the Gordian Knot: A look under the hood of ransomware attacks*. *Detection of Intrusions and Malware, and Vulnerability Assessment*, 9721, 3-24.
13. Kharraz, A., Arshad, S., Mulliner, C., Robertson, W. K., & Kirda, E. (2016). SpearPhishing: A comprehensive study on targeted phishing attacks. *Proceedings of the 2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, 1-15
14. Kharraz, A., Arshad, S., Mulliner, C., Robertson, W. K., & Kirda, E. (2016). Protection and detection of ransomware attacks. *Proceedings of the 2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, 1-16.
15. Laudon, K. C., & Laudon, J. P. (2019). *Sistemas de información gerenciales* (15ª ed.). Pearson.
16. Liao, Y., Zhao, T., Doupe, A., & Ahn, G.-J. (2016). *Ransomware: A new cyber threat to critical infrastructures*. *Proceedings of the 2016 IEEE Conference on Communications and Network Security (CNS)*, 1-9.

17. Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. Wiley
18. Mitnick, K. D. (2017). *The art of invisibility: The world's most famous hacker teaches you how to be safe in the age of Big Brother and Big Data*. Little, Brown and Company.
19. National Institute of Standards and Technology. (2012). *Computer security incident handling guide (SP 800-61 Rev. 2)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-61r2
20. National Institute of Standards and Technology. (2010). *Contingency planning guide for information technology systems (SP 800-34 Rev. 1)*. U.S. Department of Commerce. Recuperado de https://doi.org/10.6028/NIST.SP.800-34r1
21. Richardson, R., & North, M. (2017). *Ransomware: Evolution, mitigation and prevention*. *International Journal of Computer Science and Information Security*, 14(11), 45-51.
22. SANS Institute. (2023). *Incident response steps*. Recuperado de https://www.sans.org
23. SANS Institute. (2023). *Sysadmin audit: Best practices for securing your network*. Recuperado de https://www.sans.org
24. Savage, K., Coogan, P., & Lau, H. (2015). *Ransomware: A survey and analysis of the threat landscape*. *Symantec Technical Report*, 1(1), 1-21.
25. Savage, K., Coogan, P., & Lau, H. (2015). Ransomware deployment methods and analysis. *Proceedings of the 2015 IEEE International Conference on Communications (ICC)*, 1-6.
26. Shodan, D., & Badger, M. (2020). French cities exposed: A Shodan-based security study on exposed cyber assets in France. *Proceedings of the 2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, 1-12.
27. Stallings, W. (2020). *Seguridad de la información: Principios y práctica* (7ª ed.). Pearson.
28. Verizon. (2024). *Data breach investigations report (DBIR) 2024*. Verizon. https://www.verizon.com/business/resources/reports/dbir/
29. Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. Crown.