Aso Ban Caria

¿Cómo actuar ante un caso de **Ransomware?**

Autores:

Elkin Sebastian Espinosa García

Profesional Senior de la Dirección de Gestión Operativa y Seguridad – Asobancaria

Jaime Andrés Rincón Arteaga

Director de la Dirección de Gestión Operativa y Seguridad – Asobancaria

Diseño y diagramación:

Julián Andrés Rojas Castañeda

CONTENIDO

1. RESUMEN EJECUTIVO

• **Objetivo[1]:** El siguiente documento aborda las mejores prácticas y estrategias para enfrentar y mitigar los ataques de *Ransomware* en entidades bancarias y financieras. Se proporciona una guía que abarca desde la prevención hasta la respuesta eficiente ante un incidente de *Ransomware*.

• **Finalidad:** Los ataques de *Ransomware* representan una amenaza crítica para las entidades bancarias y financieras y otros sectores económicos. Esta guía se creó dada la posibilidad de pérdida o secuestro de datos sensibles, interrupción de servicios, extorsiones, entre otros.

2. INTRODUCCIÓN

"*El Ransomware es un tipo de malware que impide el acceso a la información de un dispositivo, amenazando con destruirla o hacerla pública si las víctimas no acceden a pagar un rescate en un determinado plazo*" (Incibe, 2020).

Este documento realiza un análisis sobre las mejores prácticas para mitigar casos de *Ransomware* en una organización. Asi mismo, busca establecer las acciones de prevención, mitigación y erradicación ante un incidente cibernético. En este documento encontrará los canales de comunicación ante un caso de *Ransomware*, en estos canales podrá realizar la denuncia y pedir apoyo a la Policía Nacional de Colombia, Colcert, Superintendencia Financiera de Colombia y Csirt Financiero. Así mismo, busca establecer las acciones de prevención, mitigación, erradicación y evaluación de las lecciones aprendidas y oportunidades de mejora ante un incidente cibernético.

El *Ransomware* consiste en la vulneración de la seguridad de un sistema operativo o dispositivo con el fin de secuestrar la información, bloquear aplicativos y extorsionar a la entidad bancaria con borrar o vender la información en la *dark web*[2]; este *malware*[3] es enviado principalmente a través de correos, sitios web y mensajes de texto.

A continuación, invitamos a revisar esta guía para mejorar las practicas internas sobre cómo actuar ante un caso de *Ransomware.*

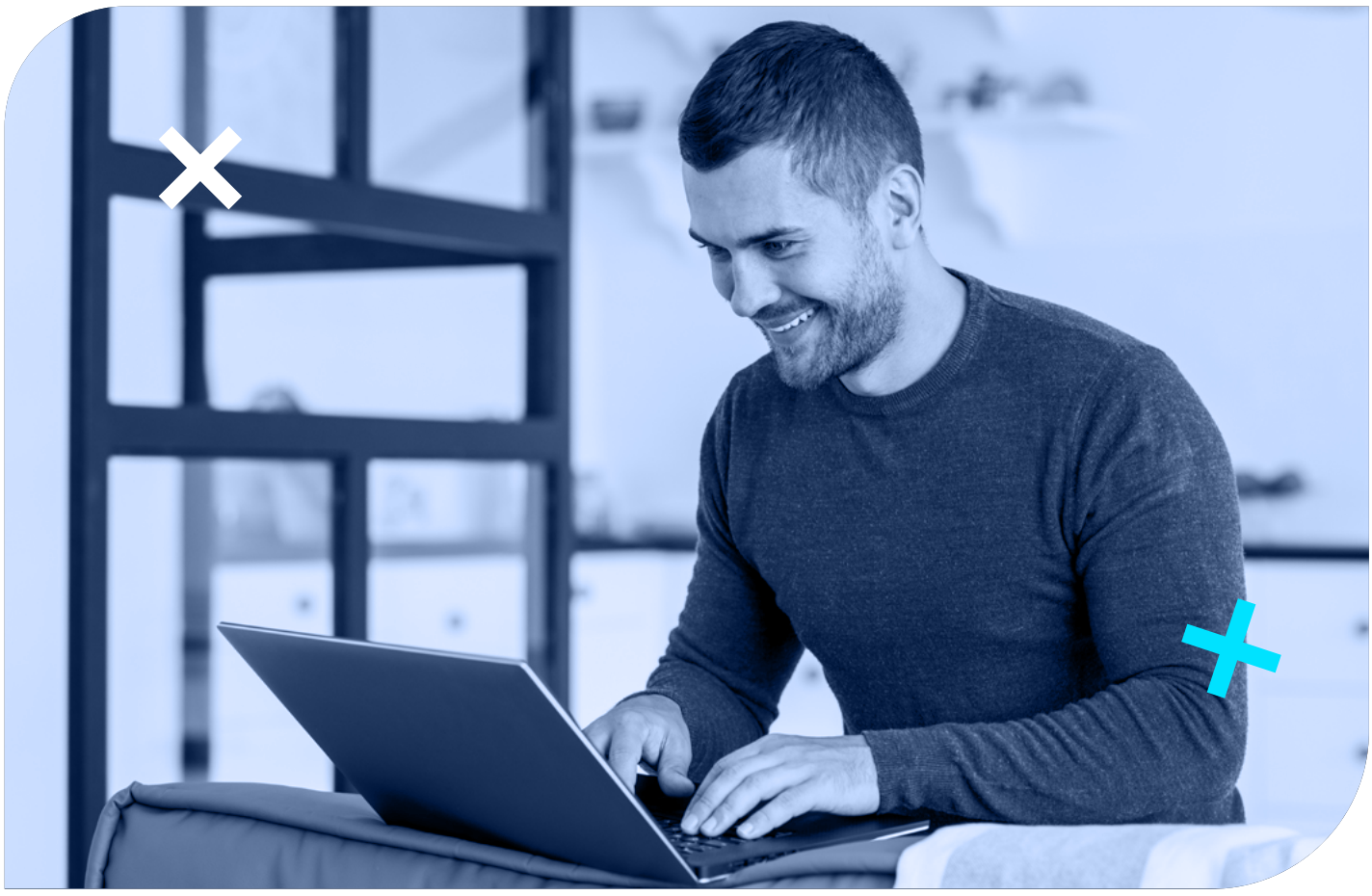
[1] El cumplimiento del objetivo está relacionado con realizar las tareas de la estructura de trabajo en el punto 8 del documento.
[2] es el conjunto oculto de sitios de Internet a los que solo se puede acceder mediante un navegador web especializado. Se utiliza para mantener la actividad de Internet privada y en el anonimato, lo que puede ser útil tanto en aplicaciones legales como ilegales. Si bien algunos la utilizan para evadir la censura del gobierno, también se sabe que se utiliza para actividades altamente ilegales. (Kaspersky)
[3] Es un término general para cualquier tipo de software con intenciones maliciosas. La mayoría de las amenazas online son algún tipo de malware.

3. DIRECTORIO

Este es el directorio de contactos ante un caso de *Ransomware*. Estos contactos tienen la finalidad de ayudar a las entidades ante un caso de *Ransomware*, sin embargo, en el punto 7.2 del documento se puede validar cuáles son los canales, medios y procedimientos para denunciar, registrar y/o notificar los casos de incidentes cibernéticos.

Los contactos para tener en cuenta son:

Actor relevante ante un caso de *Ransomware*	Correo electrónico de comunicación
Centro Cibernético de la Policía Nacional	dijin.cecip-c4@policia.gov.co
Grupo de Respuestas a Emergencias Cibernéticas de Colombia	contacto@colcert.gov.co; minticresponde@mintic.gov.co
Superintendencia Financiera de Colombia	riesgooperativosfc@entidadvigilada.com; riesgooperativo@superfinanciera.gov.co
Superintendencia Industria y Comercio de Colombia	contactenos@sic.gov.co
Csirt Financiero	reportes@csirtasobancaria.com



4. TÉRMINOS

- **Autentificación multifactor:** Es un proceso de registro en varios pasos que requiere que los usuarios ingresen más de un método de autentificación.

- **Centro Cibernético de la Policía Nacional:** Organismo policial encargado de la respuesta e investigación a incidentes cibernéticos en Colombia.

- **Cifrado:** Proceso de codificación de datos para que solo los destinatarios autorizados puedan acceder a ellos.

- **Colcert:** Grupo de Respuestas a Emergencias Cibernéticas de Colombia.

- **CSIRT Financiero:** Equipo de respuesta a incidentes de seguridad informática del sector financiero.

- **DLP (*Data Loss Prevention*):** Una estrategia para evitar la filtración de datos sensibles fuera de una organización.

- ***Firewall:*** Un sistema diseñado para prevenir el acceso no autorizado o desde una red privada al filtrar el tráfico entrante y saliente.

- **IDS (*Intrusion Detection System*):** Un sistema diseñado para detectar posibles intrusiones o violaciones de seguridad en una red o sistema informático.

- **IPS (*Intrusion Prevention System*):** Un sistema de seguridad de red diseñado para detectar y prevenir amenazas potenciales de seguridad.

- **Malware:** Es un software malicioso diseñado para infiltrarse o dañar un sistema de computadora sin el consentimiento del usuario.

- ***Ransomware:*** Es un tipo de *malware* que bloquea el acceso a la información de un dispositivo y amenaza con destruirla o hacerla pública a menos que se pague un rescate.

- **Suplantación de Identidad (*Phishing*):** Intento de obtener información confidencial suplantando a una entidad bancaria.

5. CONTEXTO

Según cifras del observatorio del delito[4], en el periodo de enero a mayo del año 2024 se realizaron 15.778 denuncias de delitos de hurto por de medios informáticos y semejantes. En comparación, en el periodo de enero a mayo del año 2023 se registraron 11.242 denuncias, con un aumento del 40,35% en Colombia. Asi mismo, en el periodo de enero a mayo del año 2024 se realizaron 5.528 denuncias de delitos de acceso abusivo a un sistema informático. En comparación, en el periodo de enero a mayo del año 2023 se registraron 4.441 denuncias, con un aumento del 24,48% en Colombia.

Por otro lado, la encuesta de ciberseguridad realizada en Asobancaria[5], en el periodo de enero a abril del año 2024 se detectaron e investigaron 8.280 casos de ciberseguridad. En comparación, en el periodo de enero a abril del año 2023 se detectaron e investigaron 7.878 casos de ciberseguridad, con un aumento del 5% de los casos de ciberseguridad en el sector financiero colombiano.

6. ¿CÓMO ACTUAR ANTES DE UN CASO DE RANSOMWARE?

A continuación, sugerimos acciones para prevenir un incidente cibernético de *Ransomware.*

6.1 Concientización del personal:

Se recomienda contar con un programa de formación para empleados en los conceptos de ciberseguridad y seguridad digital. Asi mismo, se debe integrar a los empleados nuevos en la cultura organizacional de ciberseguridad de la entidad.

Se sugiere que el programa para empleados explique las diferentes técnicas y modalidades que puede afectar la seguridad digital en la organización.

Tip: Los atacantes suelen infiltrarse engañando a usuarios, obteniendo contraseñas o induciendo a hacer clic en archivos adjuntos maliciosos o enlaces enviados dentro de los correos.

6.2 Definición de equipos de respuesta

Se recomienda definir el equipo de respuesta a incidentes donde se identifiquen roles y responsabilidades. Se sugiere que cada entidad bancaria tenga un directorio de los roles involucrados y una matriz de escalamiento según sea el caso del ataque.

Tip: La entidad bancaria y financiera debe construir un documento donde se identifique cada uno de los actores internos y externos que darán respuestas en la contención de un ataque. El documento debe tener los roles técnicos y estratégicos incluyendo el contacto de los proveedores críticos ante un incidente cibernético.

[4]Es un grupo estratégico del Área de Investigación Criminológica, encargado del monitoreo, diagnóstico, administración de la información, evaluación y análisis de la criminalidad, que tiene como propósito contribuir a la toma de decisiones y a la aplicación de acciones de las autoridades en los ámbitos internacionales, nacionales y locales, con el fin de anticipar, controlar e intervenir los delitos que afectan la seguridad y convivencia ciudadana.
[5]Esta encuesta recoge información sobre los eventos o casos de investigación de las 5 entidades bancarias y financieras más relevantes en el país.

6.3 Control de acceso de empleados

Se recomienda segmentar el control de acceso de empleados, esto permite distribuir el riesgo de un ataque y reducir el impacto de los programas que se puedan afectar ante una eventual crisis. Asi mismo, se recomienda implementar sistemas de información con autenticación multifactor.

Tip: La entidad bancaria debe realizar jornadas de cambio de contraseñas de manera periódica de acuerdo con las políticas de acceso de la organización. Asi mismo, se recomienda que la entidad bancaria defina los roles críticos de acuerdo con las funciones de cada uno de los empleados.

6.4 Mantenimiento de sistemas

Se recomienda configurar una actualización de parches y sistemas operativos de manera periódica acorde a un cronograma de actualizaciones. Asi mismo, debe tener una comunicación directa con los proveedores de servicio de los sistemas internos.

Tip: Realizar el mantenimiento regular de los sistemas de seguridad perimetral como: firewall´s[6], software de vulnerabilidades, IPS, IDS, DLP que reduzca la probabilidad de intrusión a los sistemas informáticos de la entidad. Asi mismo, se recomienda la adquisición de pólizas cyber y/o de servicios de DFIT para el monitoreo continuo de los sistemas de la entidad bancaria.

6.5 Copias de seguridad automáticas

Se recomienda auditar el funcionamiento de las copias de seguridad, estas son un recurso esencial en caso de un secuestro y/o perdida de información, estas ayudan a mitigar el impacto sobre el funcionamiento de los sistemas de operación y pérdida de información de clientes en la entidad bancaria. Asi mismo, se recomienda programar copias de seguridad de manera diaria de los aplicativos y los sistemas de información.

Es importante generar por lo menos dos copias de seguridad aisladas lógicamente y cifradas, estas copias deben ser de solo lectura e inmutabilidad de los datos.

Tip: Las copias de seguridad permiten a la entidad bancaria seguir su operación de manera funcional después de erradicar el *Ransomware* dentro de sus aplicativos o sistemas, cuando se tienen copias de seguridad aisladas que garanticen la operación con data limpia.

6.6 Comunicación interna y externa

Se recomienda construir una comunicación asertiva con empleados y actores de interés ante un caso de crisis cibernética. La comunicación es un factor clave para mantener un ambiente de confianza con el consumidor financiero. Para ello, se debe diseñar una estrategia comunicacional previa con mensajes de tranquilidad sobre los efectos del ataque cibernético, explicando las razones y efectos que puede traer la afectación.

Adicionalmente, se debe diseñar una estrategia de comunicaciones “TIPO”, donde en caso de un ataque cibernético se tengan **preparados** los mensajes internos y externos, canales de **comunicación** y el uso de los medios de comunicación **dispuestos por las entidades financieras para este tipo de escenarios.**

Tip: Se sugiere crear protocolos de comunicación por cada grupo de interés, sobre qué información comunicar que no afecte la reputación de la entidad bancaria.

[6]Son programas de software o dispositivos de hardware que filtran y examinan la información que viene a través de su conexión a Internet. Representan una primera línea de defensa porque pueden evitar que un programa malicioso o un atacante obtengan acceso a su red y a su información antes de que se produzca cualquier posible daño - McAfee.

6.7 Herramientas de mitigación

Se recomienda implementar herramientas de mitigación[7] en su esquema de prevención de seguridad digital. Las herramientas de mitigación son una barrera de entrada que tendrán los ciberdelincuentes ante una posible infectación informática de los sistemas.

Asi mismo, se recomienda tener sólidos filtros de correo no deseado y autenticar correos electrónicos entrantes, también, implementar medidas de seguridad multicapa y soluciones de seguridad avanzada, **lo que permitirá minimizar el impacto del *Ransomware* y proteger la integridad y disponibilidad de los datos.**

Tip: La entidad bancaria debe realizar pruebas recurrentes que identifiquen cuáles son los activos críticos, escala de vulnerabilidades, monitoreo constante de la red y auditoria de sistemas.

6.8 Pruebas y simulaciones de ataques cibernéticos

Se recomienda realizar pruebas y simulaciones de ataques cibernéticos que evalúen la respuesta ante una crisis cibernética, con el objetivo de identificar las fortalezas y debilidades de las organizaciones ante un eventual ataque. Estas pruebas deben estar destinadas a fortalecer la conciencia de las organizaciones, poniendo a prueba los sistemas, acciones de la organización, comunicación, entre otros. Se sugiere realizar por lo menos 1 ejercicio de respuesta a incidentes por año. Los resultados del ejercicio deben contribuir a un plan de mejora de la respuesta y contingencia ante un eventual ataque cibernético.

Tip: La simulación de crisis cibernética permite evaluar los niveles de respuesta y resiliencia de la organización ante un ataque cibernético, esto permite crear planes de acción que anticipen las actividades a realizar ante un eventual ataque cibernético.

7. ¿CÓMO ACTUAR DURANTE UN CASO DE RANSOMWARE?

A continuación, sugerimos cómo deben actuar las entidades bancarias durante un incidente cibernético de *Ransomware.*

7.1 Reporte del incidente al Equipo Directivo / Estratégico de la entidad

Una vez se identifique un ataque de tipo *Ransomware*, el equipo de SOC[8] debe validar y comprobar una real afectación del ciberataque, en este caso, se debe comunicar al cuerpo directivo de ciberseguridad de la entidad bancaria sobre el nivel de afectación. De acuerdo con el protocolo de gestión de crisis de Asobancaria, es esencial que los equipos técnicos hayan evaluado previamente: 1. Los recursos tecnológicos y procesos críticos afectados, 2. Proveedores críticos implicados en la afectación y 3. Nivel de afectación en clientes.

Estas preguntas son esenciales para evaluar el nivel de afectación de la entidad bancaria y su posible afectación sistemática.

7.2 Notificación y reporte ante un incidente cibernético

En caso de ser víctima de *Ransomware*, se debe comunicar y reportar el incidente al Centro Cibernético de Policía Nacional de Colombia, Superintendencia Financiera de Colombia, Csirt Financiero y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia, para manifestar una afectación en los sistemas de operación, aplicativos, robo de información o cualquier tipo de afectación por *Ransomware.*

Debe comunicarse para pedir apoyo en la investigación del caso a los siguientes correos:

Centro Cibernético de la Policía Nacional: dijin.cecip-c4@policia.gov.co

Csirt Financiero: reportes@csirtasobancaria.com y la línea telefónica 3174345665.

Grupo de Respuestas a Emergencias Cibernéticas de Colombia: contacto@colcert.gov.co, minticresponde@mintic.gov.co.

Recuerde que en la Superintendencia Financiera de Colombia debe comunicarse con la Delegatura de Riesgo Operacional y Ciberseguridad y con el Csirt financiero en los canales internos designados. En este sentido, los incidentes de seguridad de la información y de ciberseguridad se deben reportar al buzón riesgooperativosfc@entidadvigilada.com y al buzón riesgooperativo@superfinanciera.gov.co, empleando el protocolo de etiquetado de información y la taxonomía definidos.

Se recomienda que para ampliar la información de comunicación ante la Superintendencia Financiera de Colombia se revisen los siguientes documentos:

i. Taxonomía Única Incidentes Cibernéticos – TUIC.
ii. Circular Externa 007 de 2018.

- Recuerde que también su organización debe instaurar la denuncia ante la Fiscalía General de la Nación.

A continuación, dejamos los enlaces donde pueden ingresar para instaurar la denuncia respectiva:

i. https://sicecon.fiscalia.gov.co/denuncia/ingresoPrincipal
ii. https://caivirtual.policia.gov.co/

*Notificación a la Superintendencia de Industria y Comercio

Recuerde que en caso de que el incidente cibernético comprometa información sensible de los clientes, se debe notificar a la SIC sobre el incidente. En este sentido, debe ingresar a www.sic.gov.co en la sección de “Protección de Datos Personales” – Subsección “Sobre la protección de datos personales”. En esta sección debe acceder a incidentes cibernéticos e ingresar con los datos de usuario para registrar el incidente cibernético. A continuación, un pantallazo de la página:

Imagen 1: PASO 1: Página web de la SIC – Registro de incidente cibernético

Imagen 2: PASO 2: Página web de la SIC – Registro de incidente cibernético

Imagen 2: PASO 2: Página web de la SIC – Registro de incidente cibernético

*Notificación a redes de tarjetas y pagos electrónicos

Recuerde que, si el incidente incluye datos personales de tarjeta o información de pagos electrónicos, se debe notificar a las franquicias afectadas, siguiendo los procedimientos de cada marca. Asi mismo, si la entidad esta certificada PCI-DSS , también hay que seguir procedimientos de reporte del incidente a las franquicias asociadas de las tarjetas a través de los canales operativos de cada entidad bancaria.

7.3 Manejo de la evidencia digital

Se recomienda que, en momento de ponerse en contacto con autoridades, el equipo forense de la entidad bancaria custodie la evidencia digital para los procesos investigativos. Es importante no apagar los dispositivos comprometidos para salvaguardar la información de la memoria RAM.

7.4 Posición de la entidad bancaria ante un caso de extorsión sobre la recuperación de la información o/y funcionamiento de los sistemas informativos.

En caso de una extorsión a una entidad bancaria y/o financiera recomendamos desde Asobancaria **no pagar la extorsión**. Lo anterior, por 2 razones fundamentales: 1. La entidad bancaria no tiene garantía de que el atacante vaya a suministrar un método para desbloquear sus sistemas operativos, descifrar activos y entregar las bases de información, 2. El atacante puede usar el dinero del rescate/ extorsión para financiar ataques adicionales contra su misma organización u otras organizaciones del sector financiero u otros sectores.

La entidad bancaria y/o financiera debe comunicarse con la Dirección Antisecuestro y Antiextorsión de la policía Nacional, al correo: diase.ateci@policia.gov.co, pedir apoyo e instaurar la denuncia ante los canales anteriormente establecidos sobre el caso de extorsión. Adicionalmente, debe seguir trabajando con empresas especializadas en recuperar la información respectiva.

8. ¿CÓMO ACTUAR DESPUÉS DE UN CASO DE RANSOMWARE?

A continuación, sugerimos cómo deben actuar las entidades bancarias después de un incidente cibernético de *Ransomware.*

8.1 Aislamiento y respuesta inmediata:

Se recomienda aislar computadoras infectadas de la red para evitar la propagación. Adicionalmente, se sugiere desconectar dispositivos afectados para contener daños y facilitar la limpieza.

8.2 Gestión de copias de seguridad:

En la gestión de copias de seguridad después de un ataque de *Ransomware* es esencial cambiar contraseñas de todos los empleados de la entidad bancaria y financiera, en especial, los roles críticos dentro de la entidad. También, se debe restaurar archivos dañados de una copia de seguridad certificada que esté libre de infección.

8.3 Instalación de parches

Los equipos de seguridad y proveedores externos deben entregar un informe de vulnerabilidades sobre la afectación. En este sentido, se debe instalar los parches de seguridad que fortalezcan las deficiencias de seguridad digital, también, se debe hacer una evaluación de los sistemas corporativos comprometidos.

8.4 Acciones posteriores de la entidad bancaria ante una posible filtración de información financiera de los clientes

En primer lugar, se debe cumplir normativamente con el reporte a la Superindencia Financiera de Colombia y a la Superintendencia de Industria y Comercio. Asi mismo, frente a la afectación en los clientes, **Asobancaria sugiere realizar una campaña de comunicación de 3 pasos** para mitigar el impacto a los clientes de la entidad:

1. La entidad bancaria debe realizar un diagnóstico de la información filtrada, donde se determine cuáles fueron los clientes afectados y cuál fue el tipo de información que se filtró de la entidad bancaria y del cliente.

2. La entidad bancaria con el diagnóstico realizado en el primer paso debe construir una campaña de comunicación. La campaña realizada por la entidad bancaria debe tener el propósito de notificarle al cliente sobre la filtración de la información. La campaña puede realizarse mediante un correo electrónico y/o mensaje de texto de forma personalizada. Asi mismo, la entidad bancaria debe enviar por mensaje de texto recomendaciones para prevenir la suplantación, phishing y otros ataques que pueda recibir el cliente.

   Se recomienda a la entidad bancaria realizar una vigilancia temprana a los clientes identificados en la filtración de información. En este sentido se debe hacer un seguimiento ante movimientos sospechosos, acceso a canales digitales en dispositivos desconocidos, acceso sin identificación multifactor, cambio de contraseñas u otras acciones de riesgo de fraude.

3. Se sugiere publicar un comunicado oficial, este comunicado debe dar un mensaje de confianza sobre los clientes. El mensaje debe estar centrado a mejorar la reputación pública después del incidente cibernético.

8.5 Recomendaciones de acuerdo con el Playbook de Actuación ante *Ransomware* del CSIRT FINANCIERO

Los equipos de respuesta ante incidentes y las partes interesadas deben seguir un enfoque coherente al tratar un incidente cibernético relacionado con *Ransomware*.

Es importante que los diferentes equipos de seguridad puedan responder, movilizarse y ejecutar operaciones para limitar el impacto que pudiese tener en la marca, valor, prestación de servicios y confianza del público y clientes.

Cabe mencionar que, ante un incidente, se debe considerar la participación de los jefes de riesgos, cumplimiento, resiliencia y continuidad de negocio para que los problemas más amplios puedan gestionarse de manera eficaz y la actividad de la organización pueda continuar.

De acuerdo con el ciclo de respuesta ante incidentes y sus siete fases se contempla lo siguiente en cada una de ellas:

FASE 1 – PREPARACIÓN

En esta primera fase, los equipos de seguridad deben configurar todo de manera correcta para que no ocurra un incidente, o en caso de que ocurra se disponga de la mayor información posible en el menor tiempo aceptable.

Es importante definir un equipo de respuesta ante incidentes, el cual, debe estar compuesto por integrantes de diferentes áreas en caso de que existan.

Algunas actividades que deben realizarse en esta fase:

- Contar con un mapa de la arquitectura de la red y una CMDB (Base de datos de Gestión de la Configuración) para poder conocer en cada momento los activos que pudiesen estar infectados durante la intrusión y los lugares lógicos.
- Identificación de activos críticos para la organización. Esta información debe estar alineada con el equipo de Risk.
- Despliegue de soluciones para la detección de ataques a sistemas, tales como IDS, IPS, Email Gateway, NGFW, etc.
- Configuración de reglas y firmas en los sistemas de seguridad tanto a nivel perimetral como de monitorización, como por ejemplo Firewall y SIEM.
- Realizar actividades de hardening en los sistemas de usuarios y servidores, minimizando así los posibles riesgos en caso de incidente.
- Documentar los procesos y procedimientos de actuación ante incidentes para los diferentes equipos involucrados.

FASE 2 – IDENTIFICACIÓN

En esta fase los equipos de SOC &/o Blue Team identifican la presencia de un atacante impactando en los entornos. Esta identificación puede ocurrir por diferentes vías:

- Impacto directo sobre el equipo de un usuario, tras informar que suceden acciones extrañas en su sistema.

- Sistemas de monitorización como por ejemplo un SIEM, tras identificar una alerta de comportamiento anómalo en algún lugar de la infraestructura.
- Eventos del sistema operativo monitorizados por los equipos de seguridad, donde existe alguno que sea sospechoso.
- Correo electrónico de algún empleado de la entidad, identificando de esta manera el *Ransomware* recibido.

Algunas de estas vías nos ayudarán a identificar si existe o no un host infectado. En caso de que si, el primer paso sería el siguiente:

- Quitar el sistema infectado de la red tanto a nivel físico como a nivel lógico en caso de que esto pueda ser posible. Posteriormente, también se debería bloquear el tráfico de dicho sistema tanto de entrada como de salida.

Por último, en caso de que un sistema esté infectado, se procederá de la siguiente forma:

- Determinar el alcance que ha podido tener en la organización y el paciente cero. En muchas ocasiones, el paciente cero se podrá determinar antes de realizar las acciones de análisis, esto ayudará posteriormente a las labores del equipo de respuesta ante Incidentes ya que podrán conocer que comunicaciones ha tenido dicho host.

FASE 3 – ANÁLISIS

En el momento en que se observe la afectación por este tipo de malware es supremamente importante generar una línea de tiempo en la que se plasmen todos los eventos que se evidencien durante el análisis, algunos de los datos que debería tener en cuenta para la elaboración de la línea de tiempo sería:

- Paciente cero.
- Equipos infectados (escritorio y servidores).
- Tiempos en los que se propagó lateralmente.
- Conexiones con redes externas.
- Conexiones con redes internas.
- Si es posible, el vector de infección.
- Usuarios afectados.
- Cuentas comprometidas.
- Áreas afectadas.

Tener toda esta información completamente organizada y clara ayudará a tomar determinaciones frente al incidente y, además, permitirá tener visibilidad completa del incidente para así mismo generar un análisis de impacto y así, determinar medidas claras para la contención, mitigación y erradicación de la amenaza.

Es importante identificar el mensaje de rescate que haya dejado el cibercriminal, ya que esto puede ser una ventaja a la hora de saber cuál familia ha sido la que ha infectado el sistema.

Cuando el mensaje haya sido identificado, se pueden realizar dos comprobaciones para identificar cual ha sido la familia de *Ransomware* que ha afectado a la entidad:

1. Tomar contacto con el Csirt Financiero a través de correo electrónico reportes@csirtasobancaria.com compartiendo el mensaje que contiene el *Ransomware*.

2. Acceder a https://www.nomoreransom.org/ e introducir el mensaje de rescate para ver si el *Ransomware* se encuentra en la base de datos. También se puede ingresar a https://id-Ransomware.malwarehunterteam.com/ para cargar un archivo cifrado o la nota de rescate detectada con el fin de identificar la familia de *Ransomware*.

FASE 4 – CONTENCIÓN

En esta fase se tratan las acciones activas para mitigar el ataque. Por lo general, el objetivo aquí es que la amenaza no siga propagándose y existan nuevos equipos infectados.

- **Aislar sistemas afectados:** Desconectar las máquinas infectadas de la red para evitar la propagación del *Ransomware* a otros dispositivos.
- **Desactivar procesos maliciosos:** Identificar y detener los procesos de *Ransomware* en ejecución.
- **Bloquear comunicaciones externas:** Restringir el acceso a los servidores de comando y control utilizados por los atacantes.
- **Evaluar el alcance del ataque:** Determinar qué sistemas y datos han sido afectados.
- **Preservar evidencias:** Mantener registros y capturas de datos para análisis forense y reporte a las autoridades.

FASE 5 – ERRADICACIÓN

Durante esta fase se pretende eliminar la amenaza por completo en aquellos sistemas donde haya tenido impacto. Puede ser una fase compleja y duradera en el tiempo, dependiendo del tipo de infección.

Las acciones clave incluyen:

- **Escaneo Completo del Sistema:** Utilizar software antivirus y antimalware actualizado para realizar un escaneo exhaustivo y eliminar todos los componentes del *Ransomware*.
- **Eliminación de Archivos Maliciosos:** Borrar o aislar todos los archivos y ejecutables asociados con el *Ransomware*.
- **Reparación y Restauración del Sistema:** Arreglar cualquier daño causado por el *Ransomware*, restaurar archivos desde copias de seguridad seguras y asegurar que el sistema operativo y las aplicaciones estén actualizados.
- **Parcheo de Vulnerabilidades:** Identificar y corregir las vulnerabilidades que permitieron la infección inicial, asegurando que todos los sistemas estén parcheados y actualizados.
- **Verificación y Validación:** Realizar pruebas para asegurar que el *Ransomware* ha sido completamente erradicado y que no queda ninguna traza en el sistema.

FASE 6 – ERRADICACIÓN

El objetivo de esta fase es volver al punto de no infección sobre aquellos sistemas comprometidos para que finalmente los equipos de los usuarios o servicios vuelvan a la operación como lo hacían anterior al incidente.

Las acciones principales incluyen:

- **Restaurar Datos desde Copias de Seguridad:** Utilizar copias de seguridad limpias y seguras para restaurar los datos perdidos o cifrados.
- **Reconfigurar Sistemas y Aplicaciones:** Asegurarse de que todos los sistemas y aplicaciones estén funcionando correctamente y de manera segura.
- **Monitorear y Validar la Integridad del Sistema:** Implementar monitoreo continuo para detectar cualquier actividad sospechosa o intentos de reinfección.
- **Actualizar y Fortalecer las Medidas de Seguridad:** Revisar y mejorar las políticas de seguridad, instalar parches y actualizaciones, y fortalecer las defensas contra futuros ataques.
- **Comunicación y Reporte:** Informar a las partes interesadas sobre la recuperación y documentar el incidente y las acciones tomadas para análisis futuro y lecciones aprendidas.

FASE 7 – POST-INCIDENTE

Es importante tener disponible una base de conocimiento donde se pueda añadir toda la información de los diferentes tipos de análisis que se han hecho durante el incidente.

Tras añadir la información necesaria, mantener una reunión todo el equipo que ha formado parte de la respuesta ante incidentes también es importante, ya que a partir de dicha reunión pueden salir dos actividades:

1. Analizar los fallos que se hayan podido cometer durante el incidente, de cara a que en el futuro no vuelva a ocurrir.

2. Proponer nuevas mejoras, tanto tecnológicas como procedimentales. Puede ser que, si la organización hubiese tenido cierta tecnología, el incidente se hubiese podido erradicar desde un primer momento. Todo eso, deberá comentarse.

Posteriormente, es importante que la compañía sepa cómo se ha solucionado el incidente y si se ha hecho con éxito o no, por ello, elaborar un comunicado interno mostrará la transparencia de lo sucedido.

En último lugar, se deberán mejorar los procesos y procedimientos de respuesta ante incidentes para garantizar el éxito en cada compromiso que ocurra.

9. BIBLIOGRAFÍA

1) (Congreso de la República, 2016). Ley 1121 de 2006. Enlace: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=22647

2) (Superintendencia Financiera de Colombia). Taxonomía Única Incidentes Cibernéticos – TUIC. Enlace: https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=1049278

3) (Superintendencia Financiera de Colombia, 2018). Circular Externa 007 de 2018. Enlace: https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=1031741

4) (ONUDC, 2014). Guía para Colombia sobre el régimen jurídico contra el terrorismo y su financiación. Enlace: https://www.unodc.org/documents/colombia/2014/septiembre/GLFTweb.pdf

5) (INCIBE, 2010). Una guía de aproximación para el empresario. Enlace: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_Ransomware.pdf

6) (NextVision, 2016). Mejores prácticas para combatir una amenaza Ransomware.

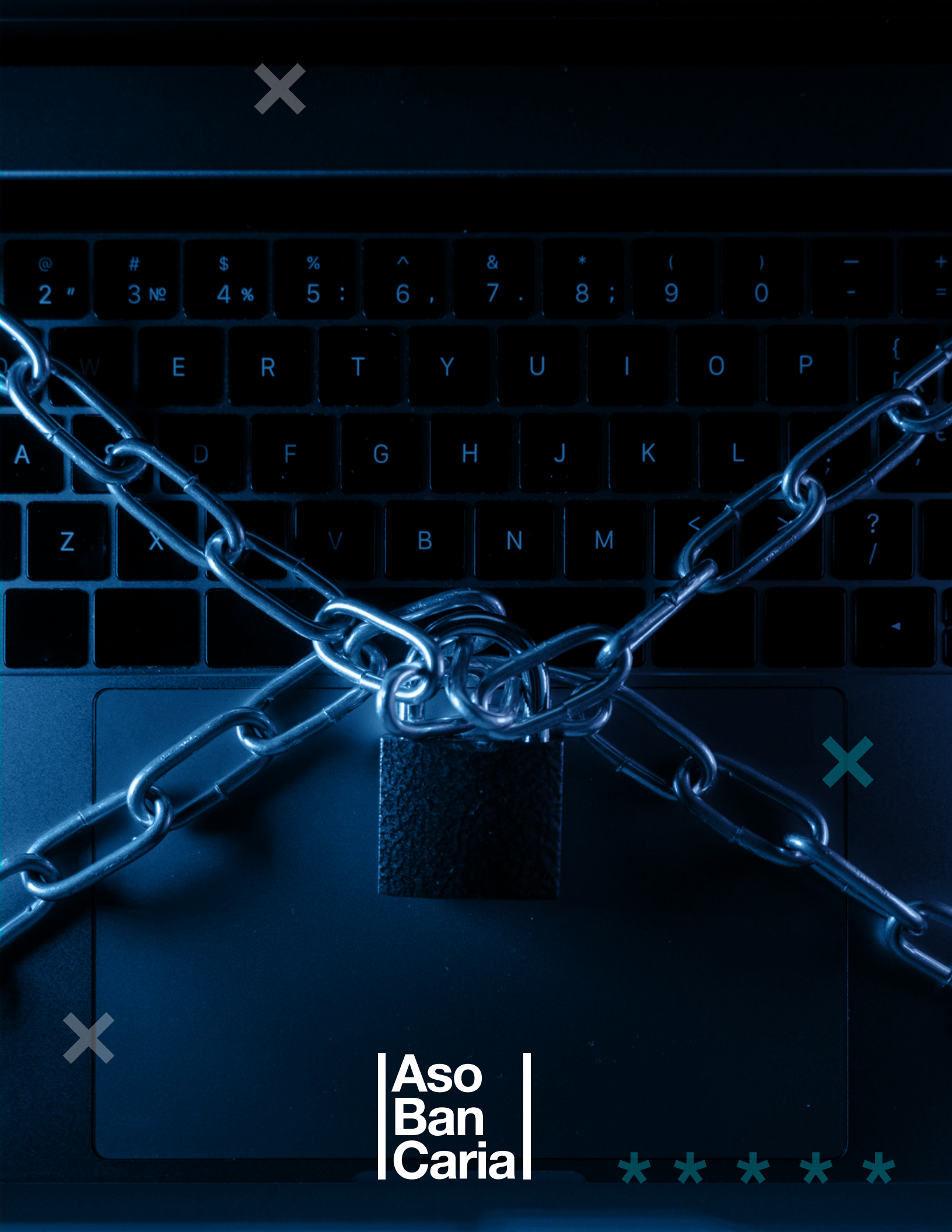
7) (Kaspersky). Buenas prácticas y consejos para protegerse del Ransomware.

8) (Sánchez, J. M.). Estrategias de protección y buenas prácticas contra ataques de Ransomware. Bogotá, Colombia.

9) Sentencia C-204/2023. Enlace: https://www.corteconstitucional.gov.co/relatoria/2023/C-204-23.htm

10) Sentencia C-205 de 2003. Enlace: https://www.corteconstitucional.gov.co/relatoria/2003/C-205-03.htm#:~:text=Sentencia%20C%2D205%2F03&text=Se%20trata%20de%20un%20tipo,cual%20se%20consuma%20el%20il%C3%ADcito.

11) (CSIRT FINANCIERO- ASOBANCARIA, 2022). INCIDENT RESPONSE PLAYBOOKS. Bogotá, Colombia.


Aso
Ban
Caria