1. **OBJETIVO GENERAL**:

Este informe de investigación presenta el análisis de las implicaciones derivadas de un ataque cibernético dirigido a las empresas municipales de Cali (Emcali). El propósito consiste en evaluar la efectividad y aplicabilidad de las políticas y procedimientos existentes de ciberseguridad, con el fin de identificar los puntos de vulnerabilidad y los controles que resultaron ineficaces en la protección de los servicios de la compañía. De igual forma se proponen diferentes soluciones efectivas que aporten a la mejora de infraestructura en Emcali con el objetivo de asegurar su capacidad de afrontar desafíos cibernéticos relacionados en el futuro.

1. **ALCANCE**

A continuación se presenta la definición del alcance del estudio, con la pregunta sobre el impacto del ataque cibernético de ransomware que sufrió la empresa Emcali el 16 de octubre de 2021.

Se tienen en cuenta diferentes aspectos para la evaluación de los procesos que fallaron para evitar este ataque, dentro de ellos se encuentran las diferentes leyes

El alcance de esta evaluación se basa en los controles de la norma técnica colombiana internacional GTC-ISO/IEC 27002:2022 que fallaron al interior de la organización.

**Normas internacionales / Frameworks / Marcos de Referencia:**

*Ley 1581 de 2012*

*Ley 1273 de 2009*

*ISO/IEC 27002*

**Proceso verificado:** Ciberseguridad

**Área:** Servicios públicos / Tecnología / Ciberseguridad

**Periodo evaluado (dd/mm/aaaa):** 16/oct/2021

1. **TRABAJO REALIZADO:**

* Se realizaron consultas a diferentes páginas las cuales notificaron qué EMCALI fue víctima de un ransomware y se pudo profundizar lo suficiente para determinar el motivo del ataque y como ocurrió.
* A partir de las consultas realizadas se pudo determinar los riesgos, amenazas, vulnerabilidades y activos, se encontró qué cuentan con 3 activos esenciales y fueron atacados por la falta de aseguramiento en las redes, también por falta de concientización por parte de los empleados.
* Se tomó como referencia la Norma Internacional GTC-ISO/IEC 27002:2022 con el fin de determinar qué controles fallaron y por qué fallaron. Se identificaron 5 controles los cuales fallaron y gracias a eso fueron un objetivo de ataque.
* Para realizar las respectivas recomendaciones de implementación de controles para mejorar se utilizó la Guía Técnica GTC-ISO/IEC 27002:2022, con estos pueden evitar qué sean tan vulnerables y la empresa optar por implementarlos para evitar pérdidas de información y pérdida de tiempo nada más en la recuperación de backups.

1. **FUENTE DE INFORMACIÓN:**

Fuentes donde se puede extraer información relevante relacionado al caso:

<https://msiamericas.com/es/la-startup-de-ciberseguridad-industrial-claroty-recauda-140-millones-en-la-ronda-2-de-financiacion-previa-a-la-salida-a-bolsa/>

<https://www.noticiasrcn.com/colombia/valle-empresa-de-servicios-publicos-de-cali-sufrio-ataque-cibernetico-391894>

<https://www.bluradio.com/blu360/pacifico/ataque-cibernetico-virus-malicioso-infecto-los-servidores-de-emcali-y-equipos-de-clientes>

1. **RESULTADOS OBTENIDOS:**
2. **Activos vulnerados:** 
   1. Servidores.
   2. Datos Sensibles.
   3. Computadores del área comercial.
3. **Riesgos**
   1. Intrusión de software malicioso.
   2. Propagación de código malicioso en la red por falta de aseguramiento.
   3. Error o fallas en los procesos operativos.
4. **Amenazas:** 
   1. Ataques de ejecución de código y/o Malware.
   2. Hurto de medios o documentos
   3. Error en el uso
5. **Vulnerabilidades:** 
   1. *Arquitectura de red insegura.*
   2. La descarga incontrolada y uso del software.
   3. La falta de conciencia de seguridad.
   4. Formación de seguridad insuficiente.
6. **Controles Existentes:**

**Entrada Física:**

* La compañía cuenta con la seguridad suficiente en cuanto al acceso físico a las sedes, cuenta con controles de entrada y está 24/7 protegido.

**Copia de seguridad de la información:**

* Emcali tiene una frecuencia establecida para hacer backups cada cierto tiempo, es por esto qué cuando ingresó el ransomware, es como si no hubiera pasado nada porque pudieron recuperar todo, gracias al último backup realizado.

**Seguridad de redes:**

* Aunque tienen controles existentes para mejorar la red y evitar posibles hackeos, cuentan con un control de redes dentro de la empresa. Cuenta con la infraestructura oportuna para protegerse de posibles hackers, pero está vez fallo por un descuido.

**Filtrado web:**

* Cuentan con acceso limitado a ciertas páginas para evitar la procrastinación de sus empleados y además paginas qué no sean seguras qué puedan ser un posible virus, son bloqueadas automáticamente.

1. **Controles que fallaron:**

| **Nro.** | **Control** | **Nombre del Control** |
| --- | --- | --- |
| 1 | 5.4 | ***Responsabilidades de la dirección*** |
| 2 | 6.3 | ***Concientización, educación y capacitación en seguridad de la información*** |
| 3 | 6.7 | ***Trabajo a distancia*** |
| 4 | 8.8 | ***Gestión de vulnerabilidades técnicas*** |
| 5 | 8.20 | ***Seguridad en redes*** |

**Matriz de Riesgos (3x3):**

| **Probabilidad** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **1 - Bajo** | El evento puede ocurrir en cualquier momento. **Al menos una vez en los últimos 2 años.** | | | | |
| **2 - Medio** | El evento puede ocurrir en cualquier momento. **Al menos una vez al año.** | | | | |
| **3 - Alto** | Se espera que el evento ocurra en la mayoría de las circunstancias. **Más de una vez al año.** | | | | |

| **Impacto / Consecuencia** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **1 - Bajo** | Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad. | | | | |
| **2 - Medio** | Si el hecho llegara a presentarse, tendría consecuencias o efectos sobre la entidad. | | | | |
| **3 - Alto** | Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad. | | | | |

| **Nivel de riesgo (Probabilidad x Impacto/Consecuencia)** | | | | **Estrategia (Asumir, Mitigar, Trasnferir, Eliminar)** | |
| --- | --- | --- | --- | --- | --- |
| **B** | **Zona de riesgo bajo(1 - 2)** | | | Asumir el riesgo | |
| **M** | **Zona de riesgo medio(3-4-5)** | | | Reducir el riesgo, evitar, compartir o transferir. | |
| **A** | **Zona de riesgo alto(6-9)** | | | Reducir el riesgo, evitar, compartir o transferir. | |

|  | | |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **\*------------ Impacto / Consecuencia -------------\*** | | |
| **BAJO** | **MEDIO** | **ALTO** |
|  | **Probabilidad** | **ALTO** |  |  | R1:Intrusión de software malicioso.  R2:Propagación de código malicioso en la red por falta de aseguramiento.  R3:Error o fallas en los procesos operativos. |
|  | **MEDIO** |  |  |  |
|  | **BAJO** |  |  |  |

**Controles recomendados a implementar:**

***5.15 Control de acceso:*** Siempre a la hora de desarrollar software para la organización lo recomendable qué aplican los expertos, es qué ese software sea auditable es decir, qué se sepa quien ingresó, cuando cerró la sesión, cuando realizó modificaciones, etc. De igual manera, auditar la parte de los controles de acceso a la red en caso tal de qué se implemente una autenticación de red. Para identificar de dónde proviene la IP y qué correo o documento de identidad está asociado a dicha IP. De está manera se lleva un control satisfactorio y evitar desorden en la organización.

***6.3 Concientización, educación y capacitación en seguridad de la información:*** El problema de Malware se originó durante la pandemia cuando diferentes funcionarios de la empresa Emcali ingresaron en correos electrónicos sospechosos lo que conlleva a la infiltración de los servidores de la compañía. Para prevenir este tipo de incidentes es fundamental promover un plan de concientización para todos los funcionarios, este plan de seguridad debe contener temáticas como fundamentos de la seguridad en línea, protección de dispositivos, comportamiento en redes sociales y sitios web y prevención de amenazas específicas.

***8.20 Seguridad en redes:*** La empresa EMCALI debe invertir en cursos robustos relacionado a la seguridad en redes para de está manera los ingenieros estén más preparados y puedan darle solución inmediata a un caso y incentivarlos a seguir mejorando en cuanto a conocimientos en cuanto a la seguridad, empezar aplicar nuevos métodos para qué no vuelva ocurrir un nuevo ataque. Qué los ingenieros se fortalezcan con cada ataque.

| **Riesgo** | **Control GTC-ISO/IEC 27002:2022** | **Hallazgo (No conformidad) / Incumplimiento) / Observación** | **Nivel de Riesgo**  (Alto /Moderado / Bajo) | **Recomendación / Oportunidad de mejora** |
| --- | --- | --- | --- | --- |
| Intrusión de software malicioso. | Gestión de vulnerabilidades técnicas. | Se abren correos de procedencia desconocida y se descargan archivos adjuntados por el atacante. | Alto | Siempre mantener el sistema operativo actualizado e invertir en un antivirus reconocido especialmente para ataques. |
| Propagación de código malicioso en la red por falta de aseguramiento. | Seguridad en redes. | Se incumple puesto a qué permitieron conectar un equipo externo a una red interconectada el cual estaba infectado y se propagó. | Alto | EMCALI debe invertir en cursos robustos relacionado a la seguridad en redes para de está manera los ingenieros estén más preparados y puedan darle solución inmediata |
| Error o fallas en los procesos operativos. | Concientización, educación y capacitación en seguridad de la información. | Los empleados no están preparados para un caso de ataque. Lo ideal sería enseñar cuales son las maneras de evitarlos para no incurrir a estos problemas contundentes. | Alto | Para prevenir este tipo de incidentes es fundamental promover un plan de concientización para todos los funcionarios, este plan de seguridad debe contener temáticas como fundamentos de la seguridad en línea, protección de dispositivos, comportamiento en redes sociales y sitios web y prevención de amenazas específicas. |

| **Nro** | **Riesgo** | **Nivel Riesgo** | **Control GTC-ISO/IEC 27002:2022** |
| --- | --- | --- | --- |
| 1 | Intrusión de software malicioso. | 🔴Alto | Gestión de vulnerabilidades técnicas. |
| 2 | Propagación de código malicioso en la red por falta de aseguramiento. | 🔴Alto | Seguridad en redes. |
| 3 | Error o fallas en los procesos operativos. | 🔴Alto | Concientización, educación y capacitación en seguridad de la información. |