**Santiago Castaño Henao - 2195304 && Juan Jose Sandoval Delgado - 2190730**

**Actividad #2 y #3 Activos de información, riesgos, amenazas, vulnerabilidades y controles**

**Instrucción:**

Teniendo clara la información clave, continúa trabajando para consolidar el contenido en un documento en donde se relacionan los activos de información, los riesgos, las amenazas, las vulnerabilidades, los controles que fallaron y las recomendaciones teniendo en cuenta las buenas prácticas de la seguridad de la información.

Posteriormente, realiza el tratamiento de los riesgos para cada uno de los controles que fallaron y define unos controles fuertes que mitiguen los riesgos existentes y realiza la exposición con tu grupo.

Para el desarrollo de esta actividad tengan en cuenta los **criterios de evaluación**:

1. Realicé otras consultas en internet sobre lo sucedido y amplié la información. Colocar la fuente de información. **(1 punto)**

Por un ataque cibernético estuvieron en riesgo los datos de las Empresas Municipales de Cali (Emcali), puesto que un virus malicioso (**RANSOMWARE**) ingresó a través de una computadora que formaba parte de una red interconectada, de esta forma se infiltraron y encriptan diferentes archivos con una contraseña, el virus deja un archivo que es donde te da las instrucciones de para qué están apuntando. Al abrir cada archivo encriptado “Dice: si quieres recuperar tus datos, escribe a uno de estos dos correos y haz un pago en Bitcoin equivalente a 50.000 a 100.000 dólares porque esta criptomoneda es más difícil de rastrear”. Con este mecanismo podría generarle grandes pérdidas a la empresa Emcali, en caso tal qué no tuvieran un backup de dicha información tendrán qué evaluar la situación para actuar de forma correspondiente.

Adicionalmente “algunos clientes recibieron un correo a nombre de Emcali con contenido adjunto que era el mismo virus, buscando que fueran descargados para robar datos de los usuarios”. De igual forma, el ataque cibernético dejó sin servicio al 30% de los clientes de Banda Ancha que la empresa tiene en la ciudad. El jefe del Departamento de Atención y Soporte al Servicio de Emcali, explicó que cerca de 28.000 equipos (routers) usados por la empresa para brindar el servicio de Banda Ancha a sus clientes se vieron afectados por este problema”

Aunque han trabajo con un grupo expertos para limpiar los equipos, el virus en muchas oportunidades se queda en estado de hibernación y ataca horas y hasta días después.

Se restableció el backup y no hubo pérdida de información, adicionalmente rápidamente se aislaron los servidores por eso solo infectan el 6% de los servidores teniendo 402 activos.

**LINKS:**

<https://www.eltiempo.com/archivo/documento/CMS-14629177>

<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. Identifique los activos, riesgos, probabilidad, impacto (Operativo, tecnológico, económico, legal, imagen reputacional, sanción o multa), que pilares de la seguridad de la información afecto (Confidencialidad, Integridad, Disponibilidad), amenazas y vulnerabilidades a los que está expuesta la organización. **(3 Puntos)**

| **Activos** | **Riesgos** | **Probabilidad** | **Amenazas** | **Vulnerabilidades** |
| --- | --- | --- | --- | --- |
| Servidores. | Intrusión de software malicioso. | ALTA | *Ataques de ejecución de código y/o Malware.* | *Arquitectura de red insegura.* |
|
| Datos Sensibles. | Propagación de código malicioso en la red por falta de aseguramiento. | ALTA | *Hurto de medios o documentos.* | *La descarga incontrolada y uso del software.* |
| Computadores del área comercial. | Error o fallas en los procesos operativos. | ALTA | *Error en el uso.* | *La falta de conciencia de seguridad.*  *Formación de seguridad insuficiente.* |

**Impacto**

***Operativo:***La entidad no puede continuar sus funciones normales puesto que los datos utilizados para esto se encuentran encriptados, mientras el grupo de TI da solución a la infiltración se detiene la operación de muchos funcionarios.

***Tecnológico****:* Hay un pérdida de datos y se compromete la confidencialidad de los mismos, hay afectación de equipos y redes en donde se ven involucrados alrededor de 28000 equipos utilizados para brindar servicio de banda ancha, esto ocasiona una interrupción del servicio y se debe aislar los servidores para evitar una mayor propagación del virus.

***Económico:***La empresa se puede ver afectada económicamente a la hora de realizar algún pago al grupo de ciberdelincuentes para la respectiva desencriptación de la información en caso tal de qué no tuvieran un respaldo.

***Legal:*** La empresa se puede ver comprometida en el factor legal por posibles fugas de información sensible por parte de los ciberdelincuentes, puede incurrir a demandas por parte de sus clientes por la filtración de sus datos personales.

***Imagen reputacional:*** A través de medios como noticieros, periódicos o redes sociales es posible qué Emcali se vea expuesto por los ataques recibidos, la imagen reputacional se verá inmediatamente afectada por falta de concientización por parte del área de TI o los mismos empleados por ausencia de conocimientos relacionado a la seguridad y como evitar posibles ataques.

***Sanción o multa:*** Se infringen las siguientes leyes lo que puede generar sanciones o multas por parte del gobierno:

**Ley 1581 de 2012, Artículo 4, numeral f):** PRINCIPIO DE ACCESO Y CIRCULACIÓN RESTRINGIDA

“El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente Ley.  
 Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley.”

**Ley 1581 de 2012, Artículo 4, numeral g):** PRINCIPIO DE SEGURIDAD

“La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.”

**Ley 1581 de 2012, Artículo 4, numeral h):** PRINCIPIO DE CONFIDENCIALIDAD

“Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.”

**Ley 1273 de 2009, artículos 269A, 269B, 269C, 269D, 269E, 269F, 269H – numeral 1,5**

**Pilares de seguridad de la información afectados**

***Confidencialidad:*** Es posible qué los atacantes hayan obtenido acceso a la información confidencial previamente a la encriptación, esto significa qué se está violando el pilar de confidencialidad ya qué pueden sobornar a la empresa por una posible publicación de esos datos sensibles o venderlo a un tercero con fines devastadores.

***Integridad:*** Es probable qué los archivos encriptados mantengan su integridad ya qué no se han alterado de forma directa. La posible violacion al pilar de integridad, es qué los sistemas y los datos hayan cambiado de cierta forma por el mismo ransomware.

***Disponibilidad:*** Los archivos y documentos esenciales para la empresa fueron encriptados por el ransomware, es decir qué se viola el pilar de disponibilidad debido a no se puede acceder a dicha información de forma inmediata, se debe realizar un pago por el respectivo rescate.

1. Teniendo en cuenta la probabilidad, el impacto y el nivel de riesgo de cada uno de los activos, se debe de realizar un mapa de calor de 3 x 3 y se debe incluir en el trabajo e informe. **(2 Puntos)**

| **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. | |

**MAPA DE CALOR**

|  | | |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **\*------------ 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** |  |  |  |

1. Identificar los controles que fallaron de la Norma Internacional ISO/IEC 27002 (Gestión de la Seguridad de la Información). Mínimo 3 y máximo 5. **(2 puntos)**

**Fallaron los siguientes controles:**

**Controles organizacionales:**

***5.4 Responsabilidades de la dirección:*** La gerencia debió exigir a todo el personal de la empresa EMCALI que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos. De igual manera no se tuvo en cuenta la planificación de proyectos para implementar los procesos y controles relacionados con la seguridad de la organización.

**Controles de personas:**

***6.3 Concientización, educación y capacitación en seguridad de la información:*** El personal de la empresa EMCALI debieron haber recibido la debida conciencia, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral.

Se puede concluir que este control no se llevó a cabo de forma correcta puesto que la forma en que el Malware se propagó fue a través de los funcionarios que no fueron cuidadosos a la hora de abrir correos y enlaces durante la pandemia.

***6.7 Trabajo a distancia:*** Emcali debió implementar medidas de seguridad durante la pandemia cuando un gran número del personal trabajaba de forma remota, esto con el fin de proteger la información a la que se accede por fuera de las instalaciones de la organización. En este caso se hubieran podido implementar medidas de seguridad como firewalls y protección contra malware, mecanismos seguros para implementar e inicializar sistemas de forma remota.

**Controles de tecnológicos:**

***8.8 Gestión de vulnerabilidades técnicas:*** La empresa no se preparó lo suficiente para posibles ataques informáticos a futuro a cualquier vector qué sean expuestos. La organización debe contar con un equipo el cual realice pruebas de bugs para de está manera parchearlos lo antes posible para evitar el uso incorrecto de los mismos. Lo ideal sería realizar diferentes simulaciones como si fueran ataques reales para analizar la situación y poder darle un solución inmediata. No tuvieron en cuenta la parte de la red interconectada, qué vulnerabilidades podría llegar a tener, no establecieron una evaluación de riesgos y monitoreo.

***8.20 Seguridad en redes:*** El área de telecomunicaciones de la empresa EMCALI no tenía controles suficientes en cuanto a seguridad de redes es por esto qué los ciberdelincuentes pudieron ingresar por este medio. No contaban con sistemas de autenticación de red es decir, qué cada empleado tenga su respectivo usuario y contraseña para ingresar a la red o si necesita ingresar con un dispositivo ajeno a la empresa, lo ideal sería solicitar una autorización al área respectiva para llevar un control y qué dichos expertos se encarguen de tomar la decisión de qué hacer, cómo conectarse a una red wifi para invitados para qué no se vea afectado el wifi operativo qué puede infectar todos los equipos organizacionales.

**5.** Con base en la Guía Técnica ISO/IEC 27002 (Código de Práctica para controles de Seguridad de la Información), se debe realizar la recomendación de controles que debe implementar la alta dirección de la organización para mitigar los riesgos identificados. **(2 puntos)**

***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.

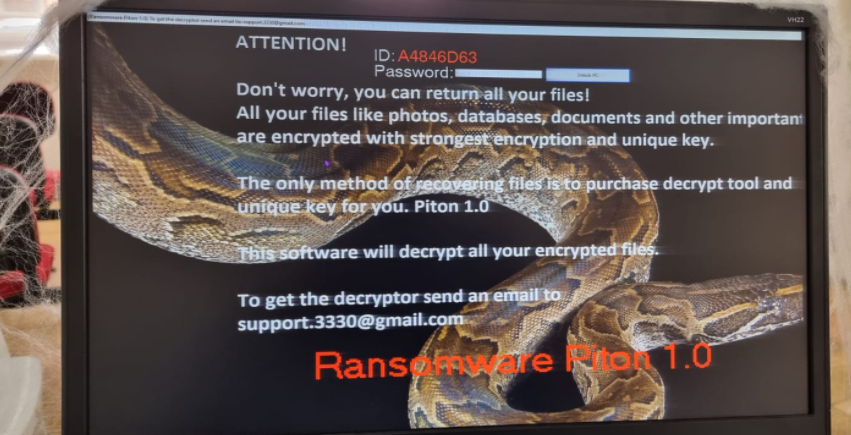
**6.** Realice un informe en Word y presente los resultados a la alta dirección (Grupo de la Especialización de Seguridad Informática) mediante presentación en power point. **(16 puntos)**

**La profundización del tema unida a su creatividad, los conducirán a superar este reto con éxito.**

**GRUPO #3 - Ataque cibernético a Emcali pone en riesgo sus datos**







**Lo que sucedió en la organización:**

*“Por un ataque cibernético se encuentran en riesgo los datos de las Empresas Municipales de Cali (Emcali), debido a que un virus ingresó a los servidores de la compañía y afectó los equipos del sistema comercial.*

*Los responsables del ataque a la base de datos estarían cobrando una suma de dinero para liberar la situación. De acuerdo con Jaime Osorio, gerente de las Tecnologías de Información de Emcali, el 16 de octubre la compañía fue víctima de un ataque de un ransomware que encripta la información de los computadores e infecta el sistema comercial.*

*“Nos reportaron un fallo en el sistema, identificamos que era un virus y encontramos un archivo en el cual informan que para entregar la llave y normalizar la situación se debe de realizar un pago con bitcoin y además de comunicarse a dos correos. La situación fue denunciada a la Fiscalía porque no vamos a realizar ningún pago”, dijo el funcionario.*

*Se conoce que la información que estaba en los computadores infectados, le cambiaron la extensión para no poder abrirlos, “tenemos todo respaldado y por eso no tenemos pérdida de archivos”, aseguró el gerente TIC.*

*Emcali también denunció que algunos clientes de la empresa de energía les ha llegado un correo electrónico a nombre de la compañía, en cual tiene un archivo adjunto que al descargarlo infecta sus equipos, por esta razón, hacen un llamado para que hagan caso omiso a correos sospechosos.*

*Al parecer la situación se registró porque gran parte de los trabajadores de Emcali por la pandemia realizaban sus actividades labores desde casa, y cuando retornaron a las oficinas, al conectarse al intranet, no fueron reconocidos por el antivirus”.*

<https://www.lafm.com.co/tecnologia/ataque-cibernetico-emcali-pone-en-riesgo-sus-datos#:~:text=Por%20un%20ataque%20cibern%C3%A9tico%20se,los%20equipos%20del%20sistema%20comercial>.