

INFORME DE

CIBERSEGURIDAD

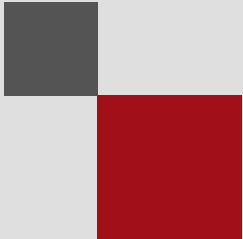


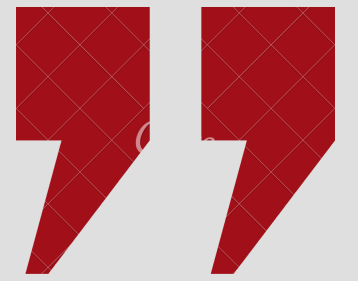
Ing. Juan José Sandoval Delgado

Ing. Santiago Castaño Henao



CONTENIDO

- Objetivo del trabajo
 - Antecedentes
 - Vector de Ataque
 - Impacto
 - Controles
 - Análisis del Ciberataque
 - Análisis de Riesgos
 - Mapa de calor
 - Framework
 - Presupuesto
 - Multas
- 



OBJETIVOS

01

Proveer contexto sobre el ciberataque realizado a la empresa Emcali.

02

Identificar los activos, amenazas y vulnerabilidades relacionados en el ataque.

03

Mostrar el impacto que tuvo el ataque en la empresa.

ANTECEDENTES DEL CIBERATAQUE

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 encriptaron diferentes archivos con una contraseña.





¿QUÉ ES EMCALI?

- Es una empresa prestadora de servicios públicos como energía, acueducto, telecomunicaciones y alcantarillado.

- Es propiedad del estado desde el 2002 y fue fundada en 1931.
- Recibe 1,79 billones de pesos anualmente.

<https://www.emcali.com.co/>

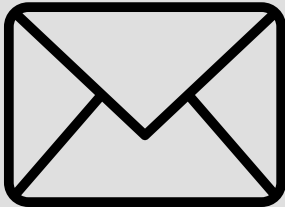
AGENTES DE AMENAZA

CIBERDELICUENTE

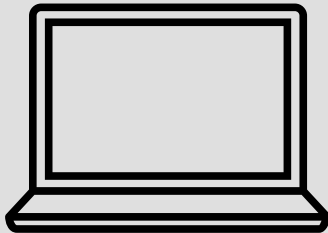


VECTOR DE ATAQUE

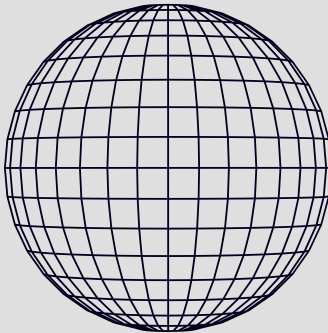
EMAILS



COMPUTADORES



RANSOMWARE EN LA RED



DEBILIDADES DE SEGURIDAD

PUNTOS DE ACCESO



CONCIENCIA EN CIBERSEGURIDAD

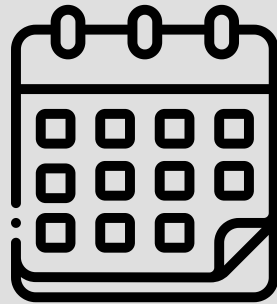


CONTROLES DE SEGURIDAD

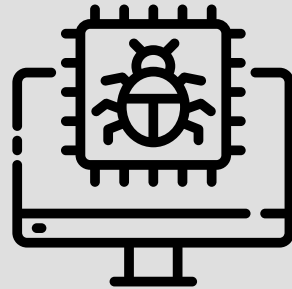
ANALISIS DE VULNERABILIDADES



REVISIONES PERIODICAS

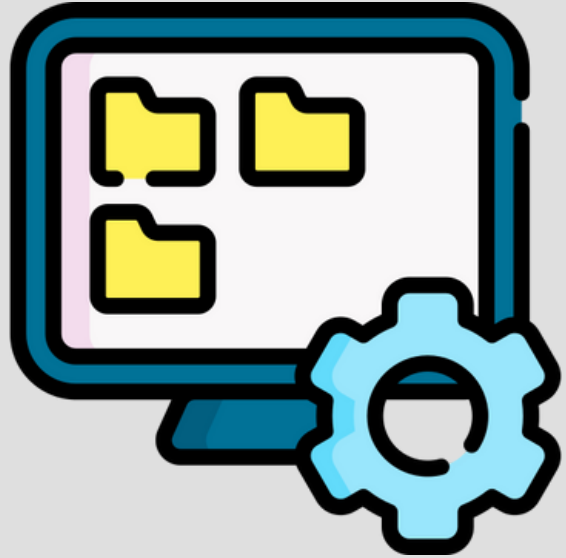


CONTROLES CONTRA MALWARE





IMPACTO”



Operativo



Económico



**Imagen
reputacional**



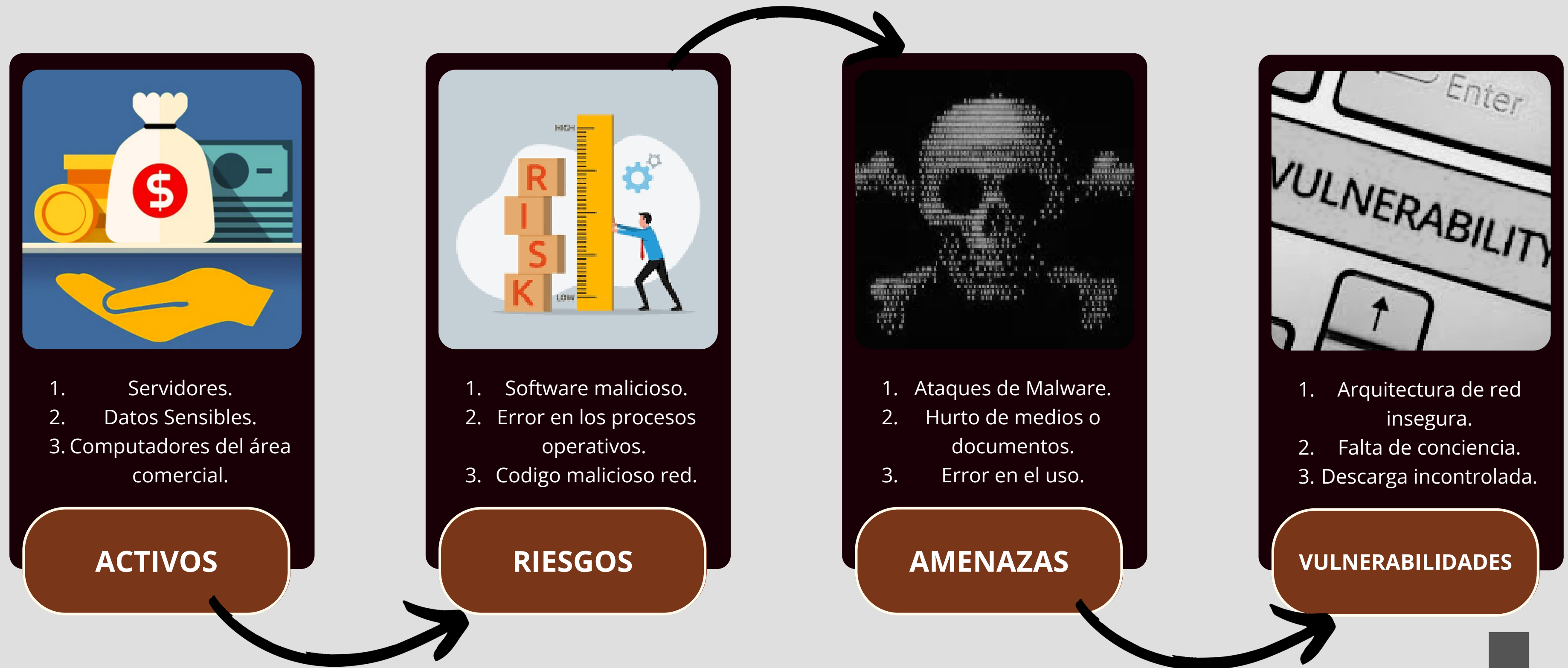
Legal



Sanciones



ANÁLISIS DEL CIBERATAQUE”



CONTROLES EXISTENTES

- **8.13** Copia de seguridad de la información.
- **7.2** Entrada Física.
- **8.23** Filtrado web.



CONTROLES QUE FALLARON

- **5.4** Responsabilidades de la dirección.
- **6.3** Concientización, educación y capacitación en seguridad de la información.
- **8.8** Gestión de vulnerabilidades técnicas.
- **8.20** Seguridad en redes.



ANÁLISIS DE RIESGOS



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.

GESTIÓN DE RIESGOS

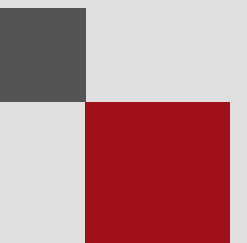
Impacto / Consecuencia	
1 - Bajo	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
2 - Medio	Si el hecho llegara a presentarse, tendría consecuencias o efectos sobre la entidad.
3 - Alto	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o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

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.

Nivel de riesgo (Probabilidad x Impacto/Consecuencia)		Estrategia (Asumir, Mitigar, Transferir, 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.

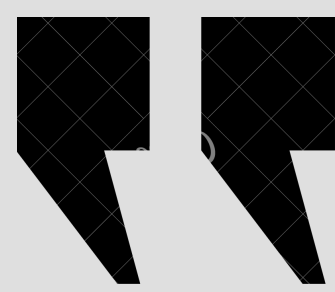
MAPA DE CALOR

		----- Impacto / Consecuencia -----		
		BAJO	MEDIO	ALTO
P r o b a b i l i d a d	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			



FRAMEWORK DE CIBERSEGURIDAD

Función	Categoría	Subcategoría	Referencias informativas
IDENTIFICAR	Evaluación de riesgos (ID.RA)	ID.RA-1: Se identifican y se documentan las vulnerabilidades de los activos.	COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-5: Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.	COBIT 5 APO12.02 ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16
PROTEGER	Concienciación y capacitación (PR.AT)	PR.AT-1: Todos los usuarios están informados y capacitados.	CIS CSC 17, 18 COBIT 5 APO07.03, BAI05.07 ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 4 AT-2, PM-13
DETECTAR	Monitoreo continuo de la seguridad (DE.CM)	DE.CM-1: Se monitorea la red para detectar posibles eventos de seguridad cibernética.	CIS CSC 1, 7, 8, 12, 13, 15, 16 COBIT 5 DSS01.03, DSS03.05, DSS05.07 NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-4: Se detecta el código malicioso.	CIS CSC 4, 7, 8, 12 COBIT 5 DSS05.01 ISO/IEC 27001:2013 A.12.2.1 NIST SP 800-53 Rev. 4 SI-3, SI-8
RESPONDER	Planificación de la Respuesta (RS.RP)	RS.RP-1: El plan de respuesta se ejecuta durante o después de un incidente.	CIS CSC 19 COBIT 5 APO12.06, BAI01.10 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8
RECUPERAR	Planificación de la recuperación (RC.RP)	RC.RP-1: El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.	COBIT 5 APO12.06, DSS02.05, DSS03.04 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8



CIS CONTROL

17.3

Cree un programa de concientización de seguridad para que todos los miembros de la fuerza laboral.

7.6

Registre todas las solicitudes de URL de cada uno de los sistemas de la organización.

8.6

Envíe todos los eventos de detección de malware.

19.1

Asegúrese de que haya planes escritos de respuesta a incidentes.



COBIT 5

APO012.01

Identificar y recopilar
datos relevantes.

APO012.02

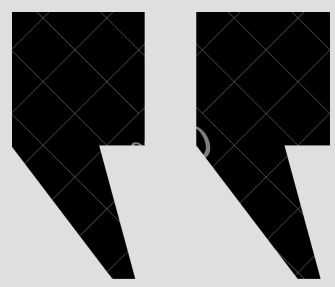
Desarrollar
información útil para
soportar las decisiones
relacionadas con el
riesgo que tomen en
cuenta la
relevancia para el
negocio de los factores
de riesgo.

APO007.03

Definir y gestionar las
habilidades y
competencias
necesarias del
personal.

DSS01.03

Supervisar las
infraestructura TI y los
eventos relacionados
con
ella.



ISO 27002:2022

8.13 - Las copias de respaldo de la información, el software y los sistemas deben mantenerse y probarse regularmente.

8.20 - Las redes y los dispositivos de red deben protegerse, administrarse y controlarse.

8,7 - La protección contra malware debe implementarse y respaldarse.

8,8 - Debería obtenerse información sobre las vulnerabilidades técnicas de los sistemas de información en uso.



NIST SP 800-53 REV4

CA-8(1)

Define los sistemas de información o componentes del sistema en donde se conducen las pruebas de penetración.

RA-3(a)

Llevar a cabo una evaluación del riesgo, incluida la probabilidad y magnitud del daño, del acceso no autorizado, uso, divulgación, interrupción, modificación o Destrucción.

AT-2(a)

Proporciona formación básica en materia de seguridad a los usuarios del sistema de información como parte de la capacitación inicial para nuevos usuarios.

CA-7(c)[1]

desarrolla una estrategia de monitoreo continuo que incluye evaluaciones de control de seguridad.

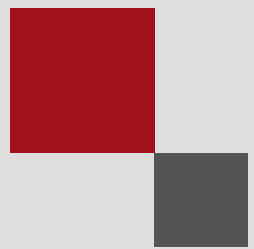


IDENTIFICAR	ESET Endpoint Security	112.000USD/Anuales
PROTEGER	ESET Endpoint Security	112.000USD/Anuales
DETECTAR	CrowdStrike Falcon	140.000USD/Anuales
RESPONDER	CrowdStrike Falcon	140.000USD/Anuales
RECUPERAR	Backblaze Business Backup	7.200USD/Anuales

PRESUPUESTO



Descripción	Cantidad	Valor Unitario	Total x Unidad	Total Anual
Software				
ESET Endpoint Security(anual), ofrece protección avanzada contra malware y ransomware.	2800	40USD	112000USD	112000USD
CrowdStrike Falcon, ofrece protección avanzada contra malware y ransomware mediante inteligencia artificial.	2800	50USD	140000USD	140000USD
Licencia Microsoft Office 365.	2800	22USD	61600USD	739200USD
Zabbix enterprise, ofrece una plataforma de monitoreo de código abierto con características avanzadas.	2800	18700USD	187000USD	187000USD
Backblaze Business Backup, ofrece planes de respaldo en la nube asequibles para estaciones de trabajo y servidores.	10	60USD	600USD	7200USD
Personal				
Gerente de Seguridad Informática	1	10000USD	10000USD	120000USD
Especialista en ciberseguridad	3	5000USD	15000USD	60000USD
Especialista defensivo	2	5000USD	10000USD	60000USD
Encargado de QA con énfasis en seguridad	1	4500USD	4500USD	54000USD
CISO (Chief Information Security Officer)	1	9000USD	9000USD	108000USD
Analista de seguridad senior	3	5000USD	15000USD	60000USD
Auditor de seguridad (por un consultor de seguridad cibernética)	2	6000USD	12000USD	72000USD
			TOTAL:	1719400USD



MULTAS

Ley 1581 de 2012

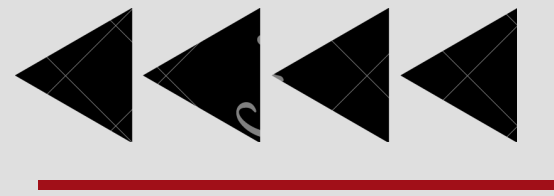
Ley 140 de 2012

- Dos mil (2.000) SMMLV.
- Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses.
- Cierre temporal de las operaciones.
- Cierre inmediato y definitivo de la operación.



- Mil (1000) SMMLV.
- Suspensión de la personería jurídica de la institución.
- Cancelación de la personería jurídica de la institución.

3'000.000.000COP



PRESUPUESTO VS MULTAS

1'719,400USD

=

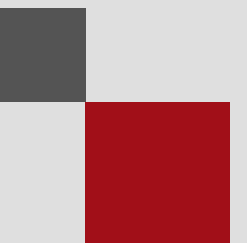
7'221,480,000COP

VS

853,782USD

=

3'000,000,000COP





¡GRACIAS!

