Agencia de Regulación y Control
de las Telecomunicaciones

Guía de Gestión de Incidentes-Ransomware

República del Ecuador

Gobierno del Encuentro | Juntos lo logramos

ÍNDICE


Análisis Inicial
Contención
Detección
Mitigación
Recuperación

ANÁLISIS INICIAL

Recopila la siguiente información

Para determinar el alcance del incidente generado por el ransomware, es importante recopilar:

1. Información de **contexto del incidente**.

2. Información técnica sobre la infección.

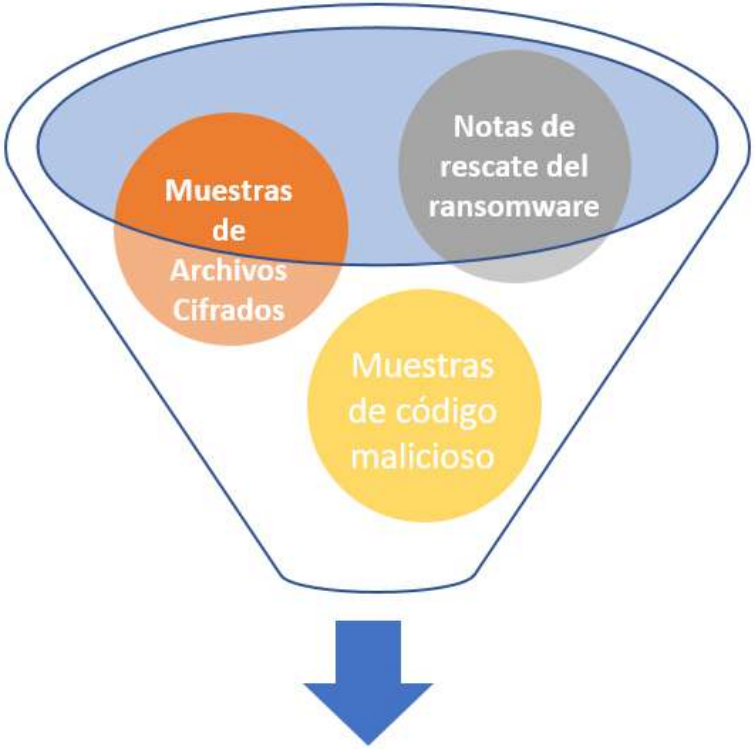
3. Información de la red en la que se ha producido la infección.

Contexto del Incidente

Es importante conocer la siguiente información:

- ¿Cuándo se produjo la infección?
- ¿Cómo se produjo la infección?
- ¿Cuántos equipos afectados tiene?
- La copia de seguridad ¿Está actualizada?
- ¿Qué acciones de mitigación tiene empleada?

Información del Incidente



Recopilar Evidencias

NOTAS DE RESCATE

Mensajes dejado por los ciberdelincuentes.

MUESTRAS DE ARCHIVOS CIFRADOS

Tamaño máximo de envío de 2 Megas

MUESTRAS DE CÓDIGO MALICIOSO

Muestras del ransomware, correo de phishing o cualquier evidencia

Información de la Red

Direccionamiento IP y Dominios

Disponer de la información actualizada.

Lista de Activos y Servidores

Disponer de la información actualizada.

Diagrama de Red

Tener la topología física y lógica actualizada .

LOGS

Información referente a Antivirus, Firewall, Anti Spam, VPN, Tráfico de información.

CONTENCIÓN DE LA AMENAZA

- Desconexión de los Equipos de Red
- Segmentación de la Red.
- Emplear los EDR disponibles
- Revisar detenidamente el tráfico de la red

DETECCIÓN DE LA AMENAZA

01

BUSCAR

Identificar la familia de ransomware implicada en el incidente, para ello:

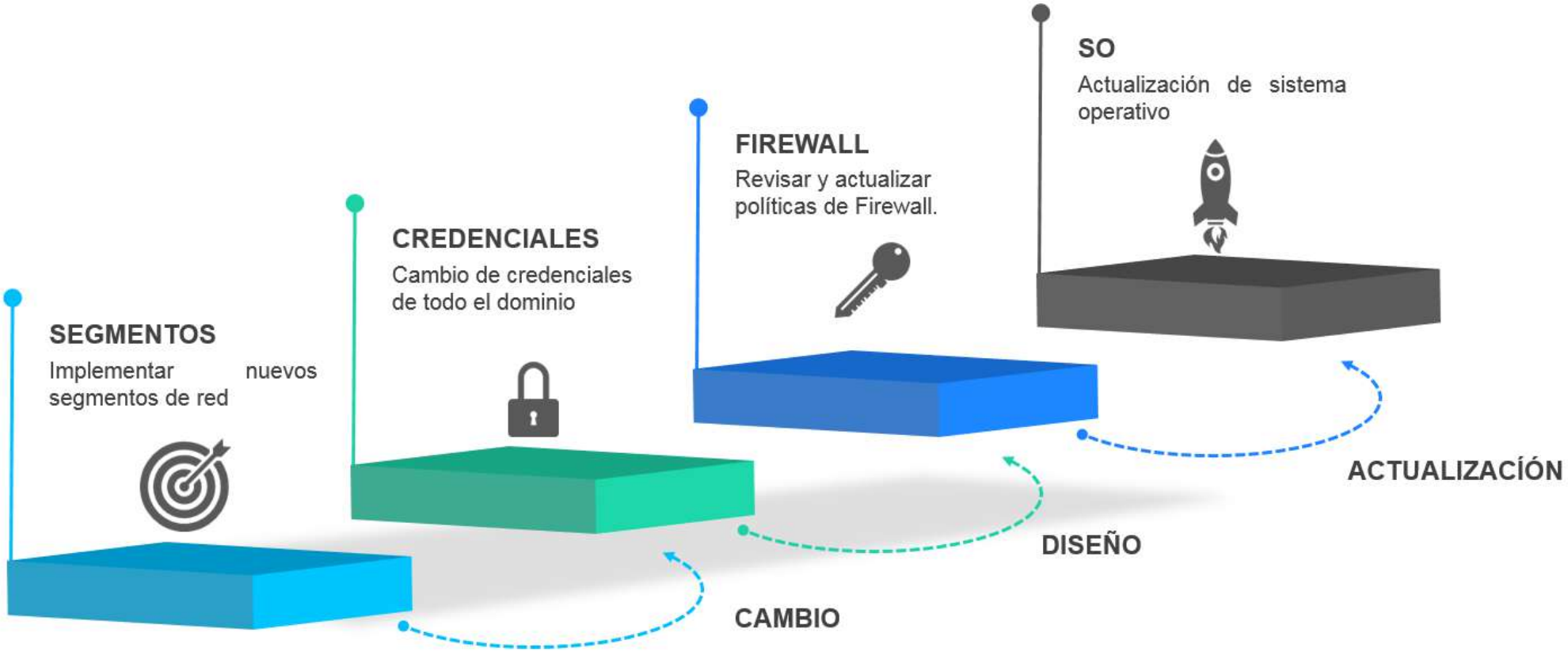
- https://id-ransomware.malwarehunterteam.com

02

Use el IDS

Desplegar esta solución en donde se tenga monitoreo del tráfico entrante y saliente

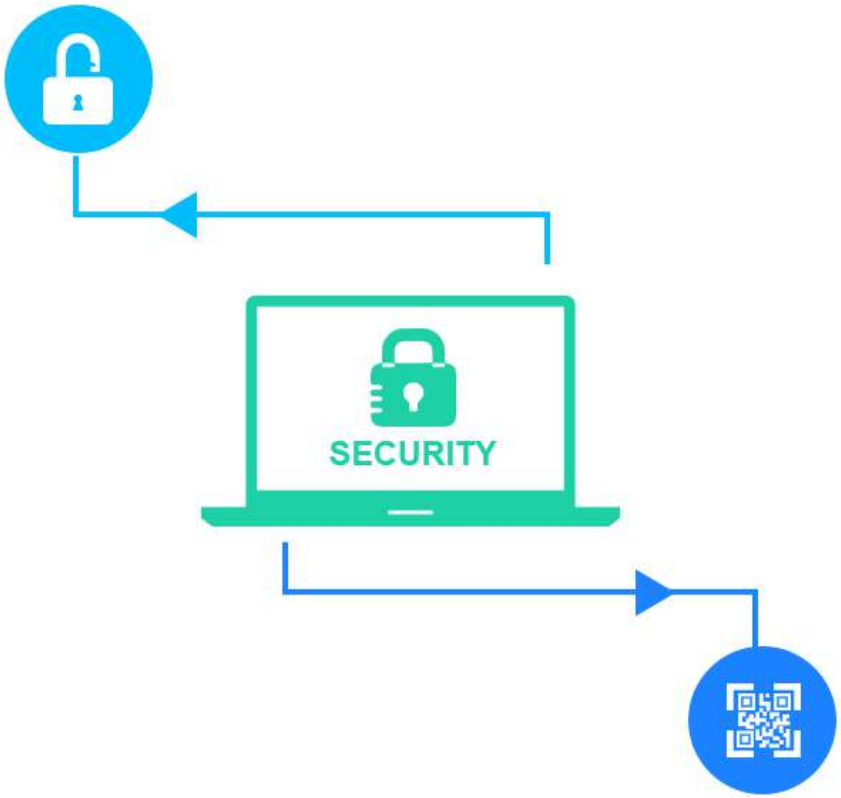
MITIGACIÓN DE LA AMENAZA



RECUPERACIÓN DE INFORMACIÓN

RESPALDOS

Si se tiene un backup (completo o parcial) del equipo afectado se sugiere: desinfectar el equipo afectado y proceder a restaurar el backup.



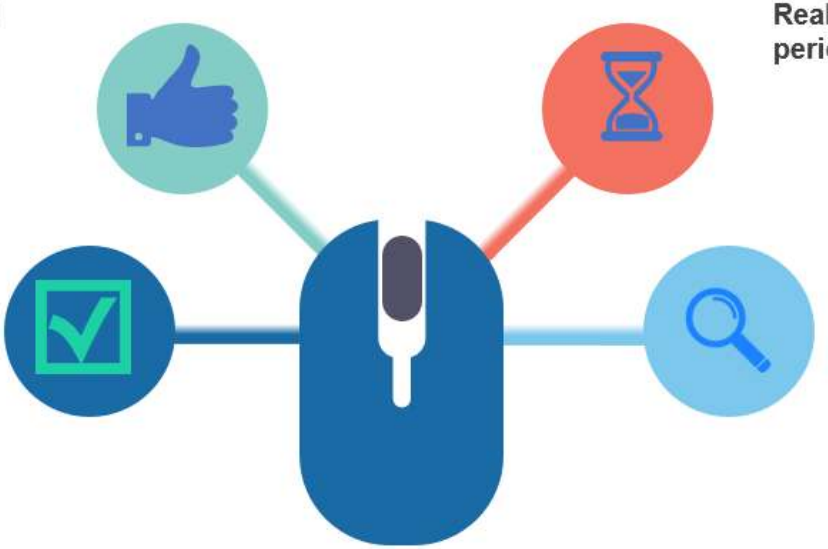
HERRAMIENTAS

En el caso de que se disponga de una herramienta para restaurar los archivos cifrados se procederá a desinfectar el equipo afectado y posteriormente se descifrará con las herramientas disponibles.

BUENAS PRÁCTICA

Definir políticas de seguridad a nivel de red.

Realizar copias de seguridad periódicamente.



Definir políticas de seguridad en el dominio

Analizar el contenido de las comunicaciones.