ALCALDÍA DISTRITAL DE CARTAGENA DE INDIAS

INFORME

2022

Alcaldía Distrital de Cartagena de Indias - Bolívar

Centro Diag. 30 # 30 - 78 Plaza de la Aduana.
(57) + (5) 6411370 - Línea Gratuita: 018000 415 393.
alcalde@cartagena.gov.co / atencionalciudadano@cartagenagov.co

Contenido

Se realizan revisiones diarias de forma automática de los servidores y equipos que aseguran el perímetro de la red de la Alcaldía Distrital de Cartagena.

Entre las actividades realizadas, estas son automáticas y se validan por el rol de soporte de seguridad, quien a su vez reporta al líder de seguridad y privacidad de la información.

Estado de Alertas de consola Sophos Central

Revisión de vulnerabilidades de los servidores.

Detalles

	Descripción	Contador	Acciones
☐	Es necesaria una limpieza manual de la aplicación maliciosa: 'ML/PE-A'	39	Marcar como resuelto
☐	Safe Browsing ha detectado un navegador en peligro	6	Marcar como resuelto
☐	Es necesaria una limpieza manual de la aplicación maliciosa: 'Mal/EncPk-ABO'	6	Marcar como resuelto
☐	Ataque detectado	3	Marcar como resuelto
☐	Error al proteger ordenador o servidor	2	Marcar como validado, Reinstalar Endpoint Protection
☐	Es necesaria una limpieza manual de la aplicación maliciosa: 'Troj/JenxLnk-G'	2	Marcar como resuelto
☐	Es necesaria una limpieza manual de la aplicación maliciosa: 'Mal/Generic-R'	2	Marcar como resuelto
☐	Es necesaria una limpieza manual de la aplicación maliciosa: 'Mal/HckPk-A'	1	Marcar como resuelto
☐	Es necesaria una limpieza manual de la aplicación maliciosa: 'Mal/Generic-S'	1	Marcar como resuelto

Informe de estado de los equipos

1156	159	203
Activo	Inactivo 2+ semanas	Inactivo 2+ meses

Detalles

- 1156 EndPoint se encuentran activos
- 159 EndPoint se encuentran inactivos entre 2 semanas y 2 meses
- 203 EndPoint se encuentran inactivas hace más de 2 meses

Informe del estado de los servidores

96	48	5	10	33
Todos	Activo	Inactivo 2+ semanas	Inactivo 2+ meses	No protegido

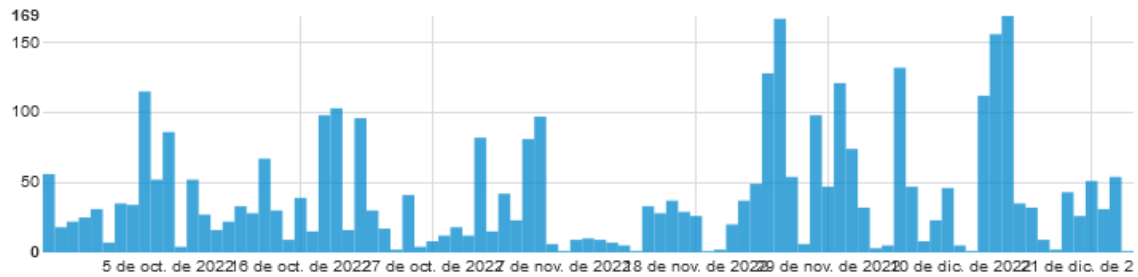
Detalles

- 23 servidores se encuentran activos.
- 15servidores se encuentran inactivos entre 2 semanas y 2 meses.
- 7 servidores se encuentran inactivos hace más de 2 meses.

De los servidores no protegido se envía relación al área de infraestructura para validar si dicho servidor ya no está en línea o fue dato de baja en el proceso de migración de la alcaldía

Informe Malware y PUA Bloqueados

Grafica trimiestral Diciembre 2022



Reporte de IPS a nivel de Firewall Fotigate 900D

Revisión de la seguridad en los equipos de la Alcaldía. Veremos a continuación algunas IP públicas con fuente de ataque hacia la entidad en la gráfica se observar el porcentaje de ataques realizados.

Víctimas de intrusión

#	Attack Victim	Counts	Critical	High	Medium	Percent of Total Attacks
1	[redacted]				19,980	23.17%
2					13,568	15.73%
3					7,780	9.02%
4					6,635	7.69%
5					5,416	6.28%
6					4,961	5.75%
7					3,320	3.85%
8					2,936	3.40%
9					2,849	3.30%
10					2,583	3.00%
11					2,282	2.65%
12					1,871	2.17%
13					1,819	2.11%
14					1,626	1.89%
15					1,540	1.79%
16					1,534	1.78%
17					1,528	1.77%
18					1,427	1.65%
19					1,388	1.61%
20					1,191	1.38%

Estos ataques son dirigidos a ciertas IP entre las cuales encontramos varias IP Internas tales como:

Top Site-to-Site IPsec Tunnels by Bandwidth

#	Site-to-Site IPsec Tunnel	Bytes	Sent	Received
1	Tig[redacted]			1.24 TB
2	VPI			844.40 GB
3	VPI			2.78 GB
4	VPI			2.53 GB
5	VPI			800.75 MB
6	VPI			537.60 MB
7	VPI			480.08 MB
8	AW			287.47 MB
9	VPI			42.61 MB
10	VPI			6.68 MB