MINISTERIO
PÚBLICO

Dirección de Tecnología de la Información y Comunicación

PGR-DTIC-0187-22

Santo Domingo, D.N.
26 de mayo 2022

A la: Consuelo Zuluaga Jordan
Encargada de Compras y Contrataciones

Asunto: Informe Pericial de la Renovación de Licencias de Soluciones Fortinet

Anexos: a. Oficio
b. Informe Pericial

Luego de extenderle un cordial saludo, nos dirigimos con la finalidad de remitirle El Informe Pericial de la Renovación de Licencias de Soluciones Fortinet. Dicha adquisición es para ser utilizada en la Dirección de Tecnología de la Información y Comunicación. Según Requisición No. 022-2959.

Contando con la debida atención que le caracteriza,

Muy atentamente,

Ing. Héctor Juan Noboa Foster
Director de Tecnología de la Información y Comunicación.

MINISTERIO PÚBLICO
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN
Santo Domingo, Rep. Dom.

MINISTERIO PÚBLICO | DEPARTA. DE COMPRAS
RECIBIDO
Fecha 26/5/2022 Hora 11:41 AM
Firma KM

MINISTERIO PÚBLICO

Dirección de Tecnología de la Información y Comunicación

Informe Pericial

Renovación licencias de soluciones Fortinet

10 de mayo 2022

MINISTERIO PÚBLICO

Dirección de Tecnología de la Información y Comunicación

Índice

MINISTERIO PÚBLICO
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN
Santo Domingo, Rep. Dom.

1. Antecedentes

En el año 2020 la Procuraduría General de la República Dominicana adquirió diferentes soluciones para robustecer la seguridad la Institución, las mismas siendo renovadas en el año 2021, entre esas están los productos de Fortinet llamadas Fortiweb, FortiMail, FortiAnalizer, FortiManager y FortiSIEM. Cada uno de ellos llevando funciones distintas para la institución.

Estas soluciones ayudan al departamento de seguridad y ciberseguridad a mantener la detección, protección y ejecución de actividades ante las distintas amenazas que recibe a diario la Procuraduría General de la República Dominicana.

Mas abajo podrá encontrar algunas estadísticas extraidas de las aplicaciones antes descritas:

FortiWeb (WAF):

El Web Application Firewall de Fortinet, protege las aplicaciones web críticas de la institución contra ataques dirigidos a vulnerabilidades conocidas y desconocidas. FortiWeb adopta un enfoque integral para proteger las aplicaciones web, incluyendo la reputación de IP, la protección DDoS, la validación de protocolos, las firmas de ataque de aplicaciones, la mitigación de bots y más para defender las aplicaciones contra una amplia gama de amenazas.

En el año 2021 este aplicativo logró detener mas 50 millones de intentos de ataques a nuestros portales web como son Portal-Servicios, SIC, Backoffice, Justicia2, entre otros.

En la ultima hora esta aplicación ha detectado y detenido unos 100 mil ataques.

#	Date/Time	Policy	Source	Destination	Threat Level	Main Type	Sub Type	HTTP Host
1	2022/05/23 14:58:39	ServerPol_Prueba	172.70.34.253	172.18.0.73		DoS Protection	Malicious IPs	mail.pgr.gob.do
2	2022/05/23 14:58:38	ServerPol_Prueba	172.70.134.246	192.168.46.30		Signature Detection	Generic Attacks(Extended)	portal.servicios.pgr.gob.do
3	2022/05/23 14:58:36	ServerPol_Prueba	172.70.135.10	172.18.0.73		DoS Protection	Malicious IPs	mail.pgr.gob.do
4	2022/05/23 14:58:36	ServerPol_Prueba	172.70.54.104	192.168.46.30		Signature Detection	Generic Attacks(Extended)	portal.servicios.pgr.gob.do
5	2022/05/23 14:58:35	ServerPol_Prueba	172.70.135.188	172.18.0.73		DoS Protection	Malicious IPs	mail.pgr.gob.do
6	2022/05/23 14:58:35	ServerPol_Prueba	172.70.135.188	172.18.0.73		DoS Protection	Malicious IPs	mail.pgr.gob.do
7	2022/05/23 14:58:33	ServerPol_Prueba	172.70.175.140	192.168.46.122		Signature Detection	Information Disclosure	justicia2.pgr.gob.do
8	2022/05/23 14:58:33	ServerPol_Prueba	172.70.174.119	192.168.46.122		Signature Detection	Information Disclosure	justicia2.pgr.gob.do
9	2022/05/23 14:58:33	ServerPol_Prueba	172.70.174.125	192.168.46.122		Signature Detection	Information Disclosure	justicia2.pgr.gob.do
10	2022/05/23 14:58:33	ServerPol_Prueba	172.70.175.164	192.168.46.122		Signature Detection	Information Disclosure	justicia2.pgr.gob.do
11	2022/05/23 14:58:32	ServerPol_Prueba	172.70.34.165	172.18.0.73		DoS Protection	Malicious IPs	mail.pgr.gob.do
12	2022/05/23 14:58:31	ServerPol_Prueba	162.158.78.229	192.168.46.6		Signature Detection	Information Disclosure	sic.pgr.gob.do
13	2022/05/23 14:58:31	ServerPol_Prueba	172.70.175.191	192.168.46.30		Signature Detection	Generic Attacks(Extended)	portal.servicios.pgr.gob.do
14	2022/05/23 14:58:31	ServerPol_Prueba	172.70.34.165	172.18.0.73		DoS Protection	Malicious IPs	mail.pgr.gob.do
15	2022/05/23 14:58:31	ServerPol_Prueba	172.70.135.74	172.18.0.73		DoS Protection	Malicious IPs	mail.pgr.gob.do
16	2022/05/23 14:58:31	ServerPol_Prueba	172.70.134.76	192.168.46.30		HTTP Protocol Constraints	Missing POST Content Type	portal.servicios.pgr.gob.do
17	2022/05/23 14:58:30	ServerPol_Prueba	172.70.34.179	192.168.46.122		Signature Detection	Information Disclosure	justicia2.pgr.gob.do
18	2022/05/23 14:58:30	ServerPol_Prueba	172.70.34.139	192.168.46.122		Signature Detection	Information Disclosure	justicia2.pgr.gob.do
19	2022/05/23 14:58:30	ServerPol_Prueba	172.70.35.48	192.168.46.122		Signature Detection	Information Disclosure	justicia2.pgr.gob.do
20	2022/05/23 14:58:30	ServerPol_Prueba	172.70.34.5	192.168.46.122		Signature Detection	Information Disclosure	justicia2.pgr.gob.do
21	2022/05/23 14:58:29	ServerPol_Prueba	172.69.33.45	172.18.0.73		DoS Protection	Malicious IPs	mail.pgr.gob.do
22	2022/05/23 14:58:29	ServerPol_Prueba	172.70.134.246	192.168.46.30		Signature Detection	Generic Attacks(Extended)	portal.servicios.pgr.gob.do
23	2022/05/23 14:58:28	ServerPol_Prueba	172.70.34.235	172.18.0.73		DoS Protection	Malicious IPs	mail.pgr.gob.do
24	2022/05/23 14:58:27	ServerPol_Prueba	172.70.175.164	192.168.46.122		Signature Detection	Information Disclosure	justicia2.pgr.gob.do
25	2022/05/23 14:58:25	ServerPol_Prueba	172.70.175.221	192.168.46.30		Signature Detection	Generic Attacks(Extended)	portal.servicios.pgr.gob.do
26	2022/05/23 14:58:23	ServerPol_Prueba	172.70.174.157	172.18.0.73		DoS Protection	Malicious IPs	mail.pgr.gob.do

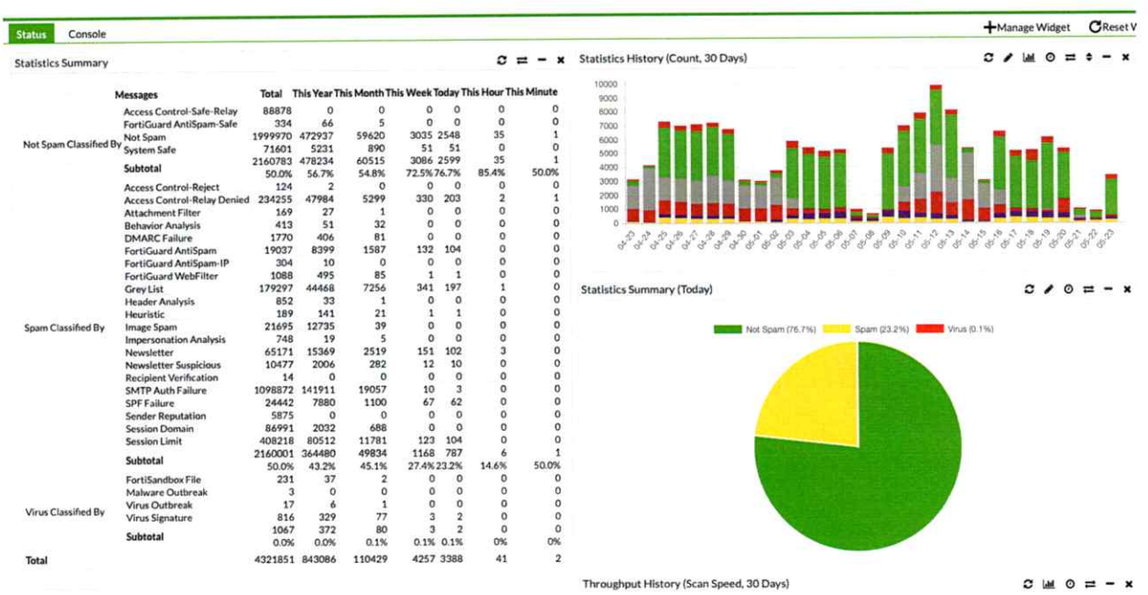
MINISTERIO PÚBLICO
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN
Santo Domingo, Rep. Dom.

FortiMail (Email Gateway):

Es un gateway seguro de correo electrónico que detiene amenazas cibernéticas basadas en volumen y dirigidas, evita la pérdida de datos sensibles y ayuda a mantener el cumplimiento de regulaciones legales.

Desde su implementación en el año 2020 esta aplicación ha detectado y detenido el 95% los correos SPAM que han querido ser entregado a la Institución, así como el 80% de los ataques de phishing.

Aquí se les presenta estadísticas con relación a los últimos 30 dias



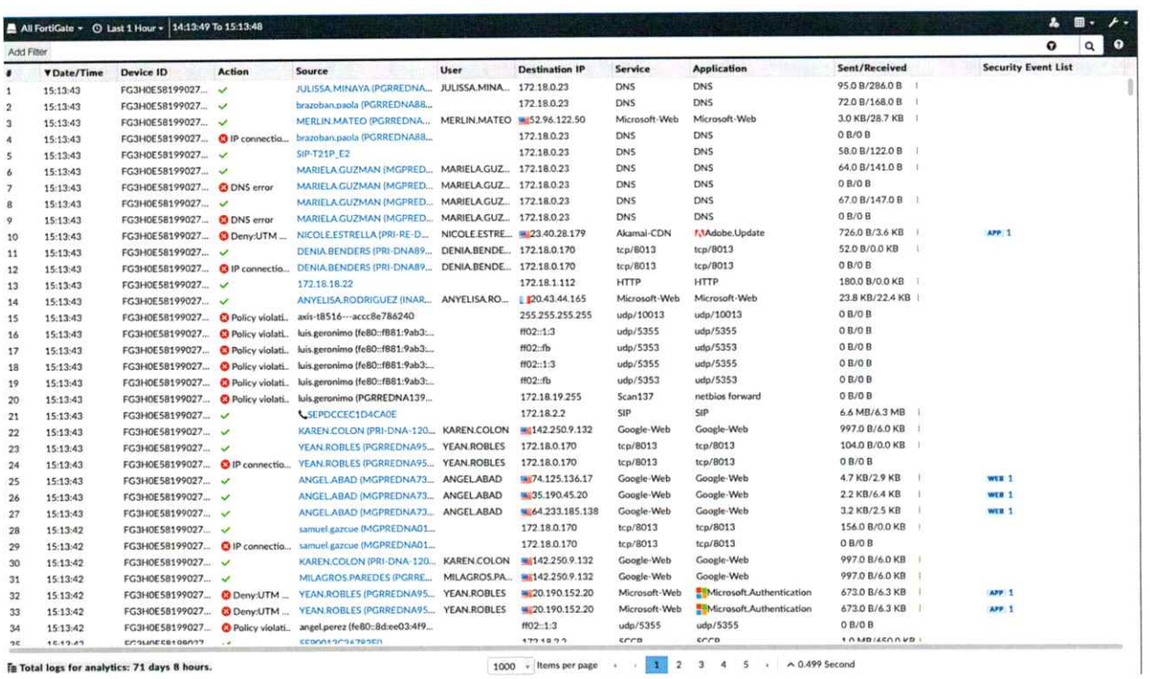
	Messages	Total	This Year	This Month	This Week	Today	This Hour	This Minute
Not Spam Classified By	Access Control-Safe-Relay	88878	0	0	0	0	0	0
	FortiGuard AntiSpam-Safe	334	66	5	0	0	0	0
	Not Spam	1999970	472937	59620	3035	2548	35	1
	System Safe	71601	5231	890	51	51	0	0
	Subtotal	2160783	478234	60515	3086	2599	35	1
		50.0%	56.7%	54.8%	72.5%	76.7%	85.4%	50.0%
Spam Classified By	Access Control-Reject	124	2	0	0	0	0	0
	Access Control-Relay Denied	234255	47984	5299	330	203	2	1
	Attachment Filter	169	27	1	0	0	0	0
	Behavior Analysis	413	51	32	0	0	0	0
	DMARC Failure	1770	406	81	0	0	0	0
	FortiGuard AntiSpam	19037	8399	1587	132	104	0	0
	FortiGuard AntiSpam-IP	304	10	0	0	0	0	0
	FortiGuard WebFilter	1088	495	85	1	1	0	0
	Grey List	179297	44468	7256	341	197	1	0
	Header Analysis	852	33	1	0	0	0	0
	Heuristic	189	141	21	1	1	0	0
	Image Spam	21695	12735	39	0	0	0	0
	Impersonation Analysis	748	19	5	0	0	0	0
	Newsletter	65171	15369	2519	151	102	3	0
	Newsletter Suspicious	10477	2006	282	12	10	0	0
	Recipient Verification	14	0	0	0	0	0	0
	SMTP Auth Failure	1098872	141911	19057	10	3	0	0
	SPF Failure	24442	7880	1100	67	62	0	0
	Sender Reputation	5875	0	0	0	0	0	0
	Session Domain	86991	2032	688	0	0	0	0
	Session Limit	408218	80512	11781	123	104	0	0
	Subtotal	2160001	364480	49834	1168	787	6	1
		50.0%	43.2%	45.1%	27.4%	23.2%	14.6%	50.0%
Virus Classified By	FortiSandbox File	231	37	2	0	0	0	0
	Malware Outbreak	3	0	0	0	0	0	0
	Virus Outbreak	17	6	1	0	0	0	0
	Virus Signature	816	329	77	3	2	0	0
	Subtotal	1067	372	80	3	2	0	0
		0.0%	0.0%	0.1%	0.1%	0.1%	0%	0%
Total		4321851	843086	110429	4257	3388	41	2

MINISTERIO PÚBLICO
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN
Santo Domingo, Rep. Dom.

FortiAnalizer:

Es una herramienta de gestión y análisis de logs que genera de manera automatizada informes configurables, posee herramientas adicionales como análisis forense, análisis de vulnerabilidades y scanning de red.

Con esta herramienta se almacena y procesa todo el trafico que pasan a través de los firewalls del fabricante Fortinet esto ayudando a la detección y corrección de fallas.

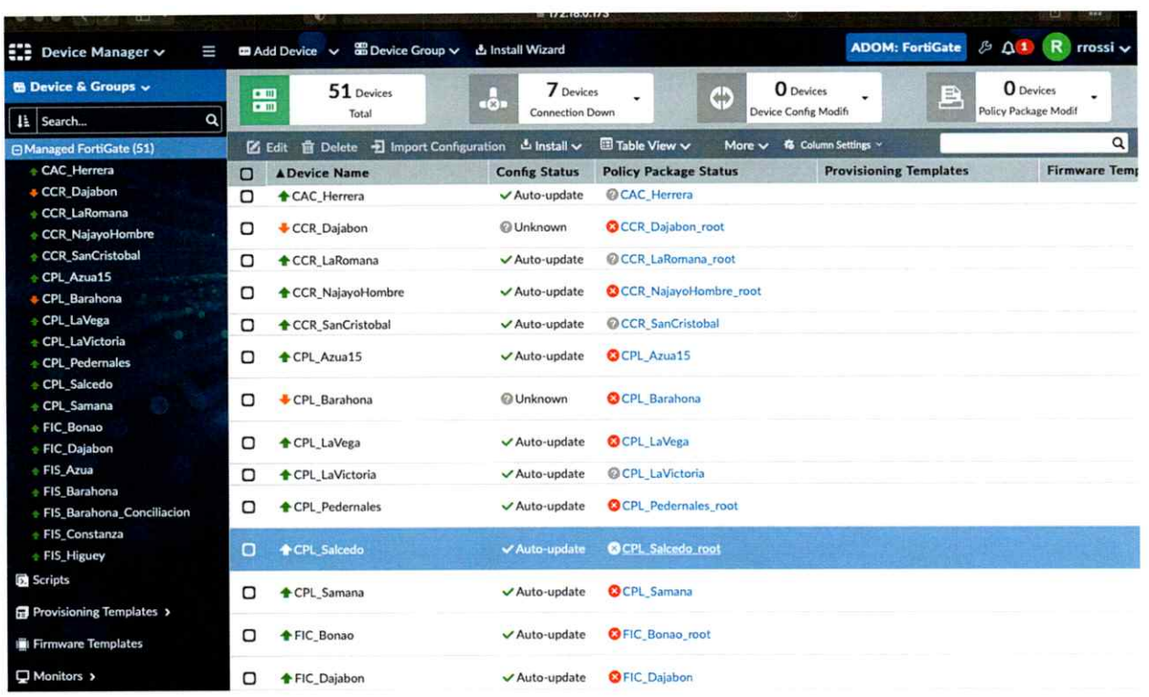


#	Date/Time	Device ID	Action	Source	User	Destination IP	Service	Application	Sent/Received	Security Event List
1	15:13:43	FG3H0E58199027...	✓	JULISSA.MINAYA (PGRREDNA...	JULISSA.MINA...	172.18.0.23	DNS	DNS	95.0 B/286.0 B	
2	15:13:43	FG3H0E58199027...	✓	brazoban.paola (PGRREDNA88...		172.18.0.23	DNS	DNS	72.0 B/168.0 B	
3	15:13:43	FG3H0E58199027...	✓	MERLIN.MATEO (PGRREDNA...	MERLIN.MATEO	52.96.122.50	Microsoft-Web	Microsoft-Web	3.0 KB/28.7 KB	
4	15:13:43	FG3H0E58199027...	✗ IP connectio...	brazoban.paola (PGRREDNA88...		172.18.0.23	DNS	DNS	0 B/0 B	
5	15:13:43	FG3H0E58199027...	✓	SIP-T21P_E2		172.18.0.23	DNS	DNS	58.0 B/122.0 B	
6	15:13:43	FG3H0E58199027...	✓	MARIELA.GUZMAN (MGPRED...	MARIELA.GUZ...	172.18.0.23	DNS	DNS	64.0 B/141.0 B	
7	15:13:43	FG3H0E58199027...	✗ DNS error	MARIELA.GUZMAN (MGPRED...	MARIELA.GUZ...	172.18.0.23	DNS	DNS	0 B/0 B	
8	15:13:43	FG3H0E58199027...	✓	MARIELA.GUZMAN (MGPRED...	MARIELA.GUZ...	172.18.0.23	DNS	DNS	67.0 B/147.0 B	
9	15:13:43	FG3H0E58199027...	✗ DNS error	MARIELA.GUZMAN (MGPRED...	MARIELA.GUZ...	172.18.0.23	DNS	DNS	0 B/0 B	
10	15:13:43	FG3H0E58199027...	✗ Deny:UTM ...	NICOLE.ESTRELLA (PRI-RE-D...	NICOLE.ESTRE...	23.40.28.179	Akamai-CDN	Adobe.Update	726.0 B/3.6 KB	APP 1
11	15:13:43	FG3H0E58199027...	✓	DENIA.BENDERS (PRI-DNA89...	DENIA.BENDE...	172.18.0.170	tcp/8013	tcp/8013	52.0 B/0.0 KB	
12	15:13:43	FG3H0E58199027...	✗ IP connectio...	DENIA.BENDERS (PRI-DNA89...	DENIA.BENDE...	172.18.0.170	tcp/8013	tcp/8013	0 B/0 B	
13	15:13:43	FG3H0E58199027...	✓	172.18.18.22		172.18.1.112	HTTP	HTTP	180.0 B/0.0 KB	
14	15:13:43	FG3H0E58199027...	✓	ANYELISA.RODRIGUEZ (INAR...	ANYELISA.RO...	20.43.44.165	Microsoft-Web	Microsoft-Web	23.8 KB/22.4 KB	
15	15:13:43	FG3H0E58199027...	✗ Policy violati...	axis-t8516---accc8e786240		255.255.255.255	udp/10013	udp/10013	0 B/0 B	
16	15:13:43	FG3H0E58199027...	✗ Policy violati...	luis.geronimo (fe80::f881:9ab3:...		ff02::1:3	udp/5355	udp/5355	0 B/0 B	
17	15:13:43	FG3H0E58199027...	✗ Policy violati...	luis.geronimo (fe80::f881:9ab3:...		ff02::fb	udp/5353	udp/5353	0 B/0 B	
18	15:13:43	FG3H0E58199027...	✗ Policy violati...	luis.geronimo (fe80::f881:9ab3:...		ff02::1:3	udp/5355	udp/5355	0 B/0 B	
19	15:13:43	FG3H0E58199027...	✗ Policy violati...	luis.geronimo (fe80::f881:9ab3:...		ff02::fb	udp/5353	udp/5353	0 B/0 B	
20	15:13:43	FG3H0E58199027...	✗ Policy violati...	luis.geronimo (PGRREDNA139...		172.18.19.255	Scan137	netbios forward	0 B/0 B	
21	15:13:43	FG3H0E58199027...	✓	SEPDCCEC1D4CA0E		172.18.2.2	SIP	SIP	6.6 MB/6.3 MB	
22	15:13:43	FG3H0E58199027...	✓	KAREN.COLON (PRI-DNA-120...	KAREN.COLON	142.250.9.132	Google-Web	Google-Web	997.0 B/6.0 KB	
23	15:13:43	FG3H0E58199027...	✓	YEAN.ROBLES (PGRREDNA95...	YEAN.ROBLES	172.18.0.170	tcp/8013	tcp/8013	104.0 B/0.0 KB	
24	15:13:43	FG3H0E58199027...	✗ IP connectio...	YEAN.ROBLES (PGRREDNA95...	YEAN.ROBLES	172.18.0.170	tcp/8013	tcp/8013	0 B/0 B	
25	15:13:43	FG3H0E58199027...	✓	ANGEL.ABAD (MGPREDNA73...	ANGEL.ABAD	74.125.136.17	Google-Web	Google-Web	4.7 KB/2.9 KB	WEB 1
26	15:13:43	FG3H0E58199027...	✓	ANGEL.ABAD (MGPREDNA73...	ANGEL.ABAD	35.190.45.20	Google-Web	Google-Web	2.2 KB/6.4 KB	WEB 1
27	15:13:43	FG3H0E58199027...	✓	ANGEL.ABAD (MGPREDNA73...	ANGEL.ABAD	64.233.185.138	Google-Web	Google-Web	3.2 KB/2.5 KB	WEB 1
28	15:13:42	FG3H0E58199027...	✓	samuel.gazcue (MGPREDNA01...		172.18.0.170	tcp/8013	tcp/8013	156.0 B/0.0 KB	
29	15:13:42	FG3H0E58199027...	✗ IP connectio...	samuel.gazcue (MGPREDNA01...		172.18.0.170	tcp/8013	tcp/8013	0 B/0 B	
30	15:13:42	FG3H0E58199027...	✓	KAREN.COLON (PRI-DNA-120...	KAREN.COLON	142.250.9.132	Google-Web	Google-Web	997.0 B/6.0 KB	
31	15:13:42	FG3H0E58199027...	✓	MILAGROS.PAREDES (PGRRE...	MILAGROS.PA...	142.250.9.132	Google-Web	Google-Web	997.0 B/6.0 KB	
32	15:13:42	FG3H0E58199027...	✗ Deny:UTM ...	YEAN.ROBLES (PGRREDNA95...	YEAN.ROBLES	20.190.152.20	Microsoft-Web	Microsoft.Authentication	673.0 B/6.3 KB	APP 1
33	15:13:42	FG3H0E58199027...	✗ Deny:UTM ...	YEAN.ROBLES (PGRREDNA95...	YEAN.ROBLES	20.190.152.20	Microsoft-Web	Microsoft.Authentication	673.0 B/6.3 KB	APP 1
34	15:13:42	FG3H0E58199027...	✗ Policy violati...	angel.perez (fe80::8d:ee03:4f9...		ff02::1:3	udp/5355	udp/5355	0 B/0 B	

FortiManager:

Es una aplicación de administración centralizada que proporcionan mando y control de las infraestructuras de seguridad basadas en Fortinet que reducen los costos de administración y los gastos generales asociados con la distribución de las actualizaciones de seguridad o la instalación de las políticas de seguridad a través de los activos administrados.

El FortiManager ayuda al departamento de seguridad de la Procuraduría General de la Republica Dominicana a tener una administración centralizada de todos los firewalls y switches Fortinet que se encuentran en la red.



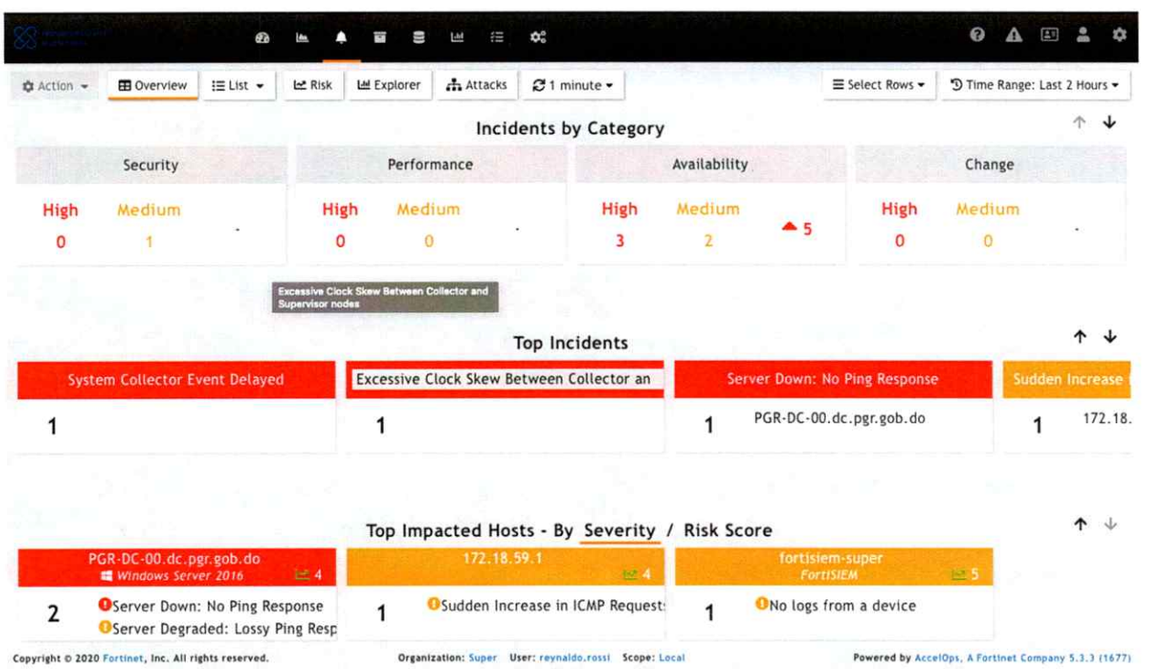
MINISTERIO PÚBLICO
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN
Santo Domingo, Rep. Dom.

MINISTERIO PÚBLICO

Dirección de Tecnología de la Información y Comunicación

FortiSIEM:
Es una aplicación que nos brinda una visibilidad completa de la red mediante: La recopilación, correlación y análisis de registros y datos de los dispositivos. Detección de anomalías y amenazas. Automatización de la respuesta y la remediación de amenazas desde un solo panel de control.

El FortiSIEM ha ayudado al departamento de seguridad a la correlación de eventos importantes para determinar posibles vectores de ataques y asi poder robustecer las políticas y configuraciones de la seguridad de la Institución.



Por todo lo antes descrito, se requiere la renovación de licencias de las soluciones de seguridad Fortinet (FortiWeb, FortiMail, FortiAnalizer, FortiManager y FortiSIEM) herramientas necesarias para fortalecer la seguridad de nuestros portales web, Correos Electrónicos, análisis de trafico y administración centralizada de los dispositivos, entre otras funcionalidades.

MINISTERIO PÚBLICO
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN
Santo Domingo, Rep. Dom.

2. Especificaciones y características del servicio.

La renovación que se está solicitando es para las soluciones de seguridad Fortinet (FortiWeb, FortiMail, FortiAnalizer, FortiManager y FortiSIEM).

A continuación, el detalle de lo requerido en este documento:

Descripción	Cantidad	Fecha de inicio	Fecha de vencimiento
FortiWeb - Firmware & General Updates - Enhanced Support - Telephone Support - Advanced Malware Protection - FortiWeb Security Service - IP Reputation - Web Application Firewall - virtual appliance for up to 2 x vCPU core	1	2022	2023
FortiMail - Enhanced Support - Telephone Support - Advanced Malware Protection - URI Click Protection - AntiSpam - FortiGuard Virus Outbreak Protection Service - FortiSandbox Cloud - Content Disarm & Reconstruction	1	2022	2023
FortiManager - Firmware & General Updates - Enhanced Support - Telephone Support - FortiManager VM license for 10 devices/domains, 1 GB/Day log and 100 GB device quota. - FortiManager VM upgrade license for 100 devices/domains, 5 GB/Day log and 1 TB device quota.	1	2022	2023
FortiAnalizer - Firmware & General Updates - Enhanced Support - Telephone Support - FortiAnalyzer VM base license for 1 GB/Day and 500 GB storage capacity -FortiAnalyzer VM upgrade license for 5 GB/Day and 3 TB storage capacity	1	2022	2023

FortiAnalizer - Firmware & General Updates - Enhanced Support - Telephone Support - FortiAnalyzer VM base license for 1 GB/Day and 500 GB storage capacity -FortiAnalyzer VM upgrade license for 5 GB/Day and 3 TB storage capacity	1	2022	2023
FortiSIEM -Firmware & General Updates - Licencia para 250 endpoints - Licencia para 1000 EPS - Indicadores de compromisos -Enhanced Support -Telephone Support -Threat Detection service	1	2022	2023

3. Análisis técnico de la solución propuesta.

La renovación que se está solicitando es para las aplicaciones de seguridad Fortinet (FortiWeb, FortiMail, FortiAnalizer, FortiManager y FortiSIEM). Los montos presupuestarios fueron basados en los precios de renovación cotizados del año 2021 y la cotización de la adquisición del FortiSIEM en el año 2021.

El suplidor del cual se utilizo los precios de referencia fue GreyMatter en cotizaciones del año 2021

Descripción	Cantidad	Precio unitario	SubTotal
FortiAnalizer	1	36,616.52	36,616.52
FortiMail	1	269,581.07	269,581.07
FortiManager	1	112,158.67	112,158.67
FortiWeb	1	176,935.31	176,935.31
FortiSIEM	1	1,812,499	1,812,499.00
		Subtotal	2,407,790.57
		Itbis (18%)	433,402.30
		Total	**2,841,192.87**

4. Conclusión.

Por lo anterior descrito Se solicita la renovación de las aplicaciones de seguridad Fortinet que posee actualmente la Procuraduría General de la Republica Dominicana Fortinet (FortiWeb, FortiMail, FortiAnalizer, FortiManager y FortiSIEM), las cuales vencen en el 23 de julio del año 2022.

5. Anexos.

1. Cotización Servicios Requeridos

Atentamente,

Hector Noboa

Gerente

Dirección de Tecnología de la Información

MINISTERIO PÚBLICO
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN
Santo Domingo, Rep. Dom.