INFORME DE EVALUACIÓN

PLAN DE CIBERSEGURIDAD PARA LA EG 2021

Plan Especializado

Elaborado por:

Gerencia de Informática y Tecnología Electoral

LIMA, AGOSTO 2021

Firma Digital
Firmado digitalmente por ROJAS BECERRA Danny David FAU 20291973851 soft
Motivo: Soy el autor del documento
Fecha: 27.08.2021 11:14:32 -05:00

Firma Digital
Firmado digitalmente por URDAY CHAVEZ Marco Antonio Alberto FAU 20291973851 soft
Motivo: Soy el autor del documento
Fecha: 27.08.2021 15:45:39 -05:00

Firma Digital
Firmado digitalmente por COTRINA CASTAÑEDA Lider Jen FAU 20291973851 soft
Motivo: Doy V° B°
Fecha: 27.08.2021 19:40:24 -05:00

Firma Digital
Firmado digitalmente por MONTENEGRO VEGA Roberto Carlos FAU 20291973851 hard
Motivo: Doy V° B°
Fecha: 28.08.2021 19:44:20 -05:00

INDICE

LISTADO DE ABREVIATURAS

Equipo de Respuesta ante Incidentes de Ciberseguridad	CSIRT
Firewall de aplicaciones web	WAF
Gerencia de Informática y Tecnología Electoral	GITE
Jurado Nacional de Elecciones	JNE
Oficina Nacional de Procesos Electorales	ONPE
Presidencia de Consejo de Ministros	PCM
Policía Nacional del Perú	PNP
Registro Nacional de Identificación y Estado Civil	RENIEC
Sistema de Prevención de Intrusos	IPS
Elecciones Generales 2021	EG 2021

I. RESUMEN EJECUTIVO

La finalidad del presente informe es la ejecución de la tarea “Evaluar el Plan de Ciberseguridad para las Elecciones Generales 2021”; conforme a la formulación establecida en el POE EG 2021 V00 con Resolución Gerencial N° 000002-2021-GITE/ONPE.

La finalidad de la presente evaluación es verificar si se logró asegurar los sistemas informáticos de la entidad y asegurar la información generada en el marco de las Elecciones Generales 2021.

Damos cuenta que, durante el proceso electoral, las herramientas detectaron y mitigaron todos los eventos de Ciberseguridad como fueron: infección de malware, correos spam, indisponibilidad de servicio, accesos no autorizados, entre otros utilizando técnicas de análisis de comportamiento, bloqueos de listas negras o inteligencia de amenazas. Y no se registraron incidentes que ocasionaron alguna indisponibilidad o degradación de los servicios que dan soporte a la EG 2021, permitiendo el normal funcionamiento de todos los sistemas.

II. EVALUACIÓN DE ACCIONES Y/O ACTIVIDADES OPERATIVAS, TAREAS, PROYECTOS

2.1 Descripción de acciones

En el numeral VIII. Acciones del Plan de Ciberseguridad para la EG 2021, se establece lo siguiente:

3. Cód.	4.Actividad Operativa / Tarea / Acción	Descripción
1	Monitorear las herramientas de Ciberseguridad.	Verificar la mitigación de eventos de Ciberseguridad en las herramientas para evaluar una mejora en las políticas de bloqueo.
2	Gestionar servicios relacionados a Ciberseguridad.	Gestión del servicio contratado de Ethical Hacking el cual permite detectar vulnerabilidades en los sistemas.
3	Coordinar reuniones semanales con los integrantes del CSIRT Electoral.	Efectuar reuniones semanales con integrantes de PCM, JNE, RENIEC y sus proveedores para intercambio de información de amenazas que atentan contra los sistemas de las instituciones involucradas en el proceso electoral y su procedimiento de mitigación.
4	Realizar el seguimiento al monitoreo efectuado por los integrantes del CSIRT Electoral.	Seguimiento a las alertas remitidas por los integrantes de PCM, JNE, RENIEC y sus proveedores, en el grupo de mensajería instantánea, para evaluar su escalamiento y toma de acción en ONPE.

Tabla N° 1: Lista de actividades del Plan de Ciberseguridad para la EG 2021

Al respecto, en cumplimiento con las actividades señaladas, en la siguiente tabla se indican las acciones realizadas:

	FORMATO	Código:	FM11-GPP/PLAN
ONPE	EVALUACIÓN DE PLANES ESPECIALIZADOS Y DE ACCIÓN	Versión:	01
		Fecha de aprobación:	03/01/2017
		Página:	1 de 1

1. NOMBRE DEL PLAN - AÑO: Plan de Ciberseguridad EG 2021

2. ORGANO RESPONSABLE: Gerencia de Informática y Tecnología Electoral

3. Cód	4.Actividad Operativa / Tarea / Acción	5. Unidad Orgánica Responsable	6. Unidad de Medida	7. Sustento	8. FECHA PROGRAMADA		9. FECHA EJECUTADA		10. METAS FÍSICAS MENSUALES										11. MEDICIÓN DEL AVANCE DEL PROCESO EVALUADO			12. ANALISIS CUALITATIVO		
					Inicio	Fin	Inicio	Fin	Feb 2021		Mar 2021		Abr 2021		May 2021		Jun 2021		META PROGRAMADA	META EJECUTADA	% AVANCE	DESCRIPCIÓN DEL AVANCE / CUMPLIMIENTO	DIFICULTADES PRESENTADAS	MEDIDAS CORRECTIVAS
									Pr	Ej	Pr	Ej	Pr	Ej	Pr	Ej	Pr	Ej						
III	PROCESOS DE SOPORTE																							
3.3	PROCESO: GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN																							
	ACTIVIDAD: Dar soporte a la institución en temas relacionados a las tecnologías de la institución.																							
1	Monitorear las herramientas de Ciberseguridad.	SGIST	Reporte	Reporte	01/02/21	30/06/21	01/02/21	30/06/21	1	1	1	1	1	1	1	1	1	1	5	5	100%	**Febrero 2021:** De forma diaria se realizó el monitoreo de las herramientas de Ciberseguridad detectándose 1,412,589 eventos. **Marzo 2021:** De forma diaria se realizó el monitoreo de las herramientas de Ciberseguridad detectándose 322,547 eventos. **Abril 2021:** De forma diaria se realizó el monitoreo de las herramientas de Ciberseguridad detectándose 8,446,751 eventos. **Mayo 2021:** De forma diaria se realizó el monitoreo de las herramientas de Ciberseguridad detectándose 161,932 eventos. **Junio 2021:** De forma diaria se realizó el monitoreo de las herramientas de Ciberseguridad detectándose 735,912 eventos.	ninguna	ninguna
2	Gestionar servicios relacionados a Ciberseguridad.	SGIST	Reporte	Reporte	01/02/21	31/05/21	01/02/21	31/05/21	1	1	1	1	1	1	1	1			4	4	100%	**Febrero 2021:** Con Informe: 000023-2021-DRB-SGIST-GITE (19FEB2021), Se remitió pliego de consultas con respuestas y TDR modificado del SERVICIO DE ETHICAL HACKING – EG 2021. Con Informe: 000026-2021-DRB-SGIST-GITE (26FEB2021), En el marco del Servicio Ethical Hacking EG 2021, se verificó que las propuestas de los postores Kunak Consulting S.A.C. y Strategos y Asociados S.A.C. se encuentran conforme a lo indicado en TDR. **Marzo 2021:** Con Informe: 000027-2021-DRB-SGIST-GITE (17MAR2021), se solicitó un personal adicional para el Servicio Ethical Hacking EG 2021. Con Informe: 000029-2021-DRB-SGIST-GITE (19MAR2021), se emitió la conformidad por el entregable del Servicio Ethical Hacking EG 2021. **Abril 2021:** Se realizó la ejecución del servicio Ethical Hacking EG 2021 que consistió en buscar vulnerabilidades en sistemas informáticos **Mayo 2021:** Informe: 000033-2021-DRB-SGIST-GITE (10MAY2021), se emitió la conformidad por el 1er y 2 do entregable del Servicio Ethical Hacking EG 2021.	ninguna	ninguna
3	Coordinar reuniones semanales con los integrantes del CSIRT Electoral.	SGIST	Reporte	Reporte	01/02/21	31/03/21	01/02/21	31/03/21	1	1	1	1	-	1	-	1	-	1	2	5	250%	**Febrero 2021:** Se realizó la reunión de coordinación de plan de acción de incidentes realizada el 11FEB2021 Se continuó con la reunión de coordinación de plan de acción de incidentes realizada el 13FEB2021 Reunión de coordinación realizada el 22FEB2021 con especialistas de las entidades y los proveedores ISP. Reunión de coordinación general realizada el 25FEB2021 para la gestión de incidentes ejecutada por los proveedores ISP. **Marzo 2021** Se realizaron las siguientes reuniones El 01MAR2021 con especialistas de las entidades y los proveedores ISP para planificar de Ciberejercicios. El 02MAR2021 para analizar la gestión de incidentes de Ciberseguridad en cada entidad. El 04MAR2021, para dar a conocer las Ciberamenazas durante elecciones. El 09MAR2021, para presentar la metodología del CSIRT. El 25MAR2021, para presentar la matriz de contactos. **Abril 2021:** Reunión realizada el 01ABR2021, para elaborar la matriz de activos críticos. **Mayo 2021:** Reunión de coordinación general realizada el 13MAY2021, donde se indicaron procedimientos de mitigación de software malicioso. Reunión de coordinación general realizada el 20MAY2021, donde se indicaron los tipos de ataques que provocan una posible denegación de servicio de los sistemas web publicados en Internet. Reunión de coordinación general realizada el 27MAY2021, donde se aclararon los contactos de escalamiento en caso ocurra un incidente de Ciberseguridad. **Junio 2021:** Se realizó la reunión de coordinación general realizada el 24JUN2021, donde se expuso las mitigaciones que se realizaron a nivel de los activos publicados a Internet durante las EG 2021.	ninguna	ninguna
4	Realizar el seguimiento al monitoreo efectuado por los integrantes del CSIRT Electoral.	SGIST	Reporte	Reporte	01/04/21	30/06/21	01/04/21	30/06/21	-	1	-	1	1	1	1	1	1	1	3	5	167%	**Febrero 2021:** Se detectaron 04 eventos relacionados a filtración de datos, privacidad de chats, ciberataques y denegación de servicio. **Marzo 2021:** Se detectaron 04 eventos relacionados a fuga de información en redes sociales, amenazas de ataque informático, ciberataques, problemas en sistemas de autenticación. **Abril 2021:** Se detectaron 04 eventos relacionados filtración de datos, difusión de noticas maliciosas, bloqueo de emails, ransonware. **Mayo 2021:** Se detectaron 04 eventos relacionados ciberataques, campaña de pishing, VMware, campaña de malware. **Junio 2021:** Se detectaron 04 eventos relacionados difusión de noticias maliciosas, alerta de ataque a entidades del gobierno peruano, correos maliciosos, difusión de noticias maliciosas.	ninguna	Ninguna

Tabla N° 2: Evaluación de las actividades del Plan de Ciberseguridad para la EG2021

A continuación, se detallan las acciones realizadas por cada actividad:

Actividad 1: Monitorear las herramientas de Ciberseguridad.

Acciones realizadas:

Durante el mes de mayo y junio se realizó el monitoreo de los eventos detectados y mitigados por las herramientas de Ciberseguridad que protegieron la integridad, confidencialidad y disponibilidad de los sistemas que dieron soporte a las elecciones. A continuación, se muestra en una tabla que consolida los eventos registrados desde el inicio del servicio de monitoreo de las aplicaciones electorales publicadas a Internet:

Eventos detectados y bloqueados						
Herramienta	Febrero	Marzo	Abril	Mayo	Junio	Suma de eventos
Sistema de prevención de Intrusos (IPS)	1.545	7.991	4.432	16.861	1.067	**31.896**
Monitoreo Antimalware y antispam Office 365	*	2.692	13.724	18.670	1.327	**36.413**
Firewall Perimetral	*	*	1.799	17.226	6.933	**25.958**
Anti-Denegación de Servicio	*	*	1	*	*	**1**
Firewall de Aplicaciones Web Cloud	*	*	8.250.000	21.960	653.260	**8,925,220**
Firewall de Aplicaciones Web On premise	1.411.044	311.864	176.795	87.185	73.300	**2,060,188**
Antimalware (Antivirus)	*	*	*	30	25	**55**
					Total de Eventos	**11,079,731**

Tabla N° 3: Total de 11,079,731 eventos detectados y mitigados por las herramientas de Ciberseguridad.

A continuación, se presenta el detalle de la detección y mitigación en cada herramienta de Ciberseguridad:

- Monitoreo del Sistema de prevención de Intrusos (IPS):

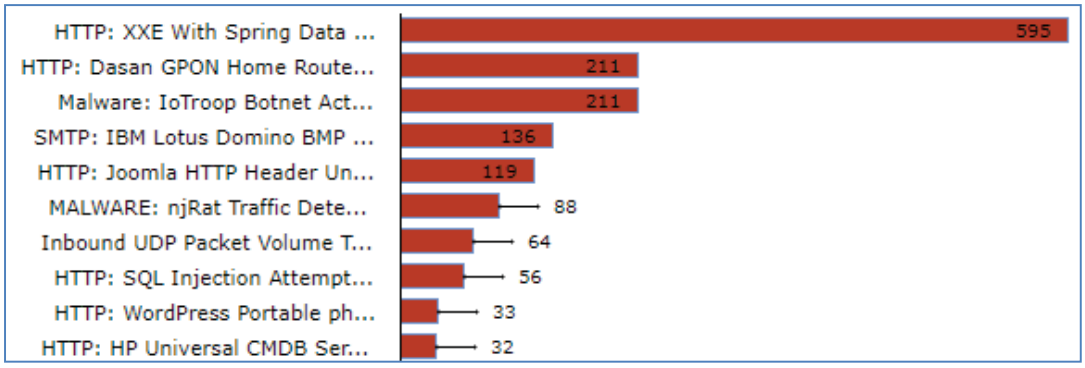


Figura N° 1: Se observa un total de 1.545 eventos detectados y mitigados por la herramienta IPS durante el mes de febrero.

* Sin registro de eventos

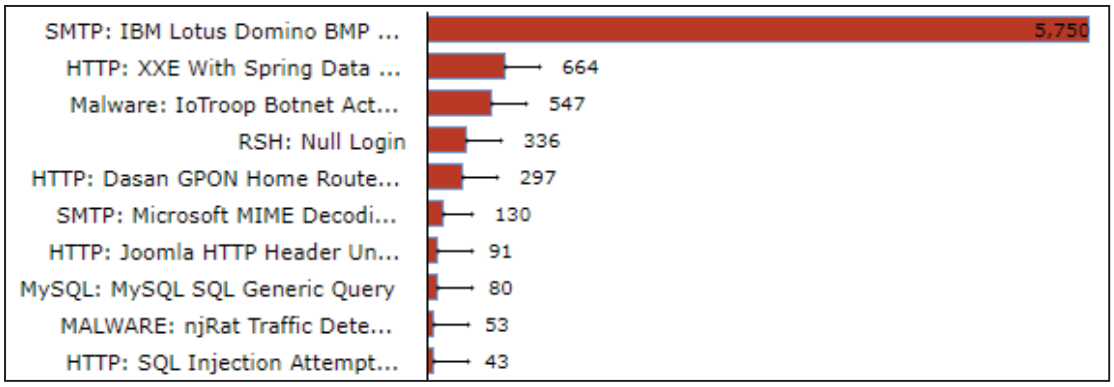


Figura N° 2: Se observa un total de 7.991 eventos detectados y mitigados por la herramienta IPS durante el mes de marzo.

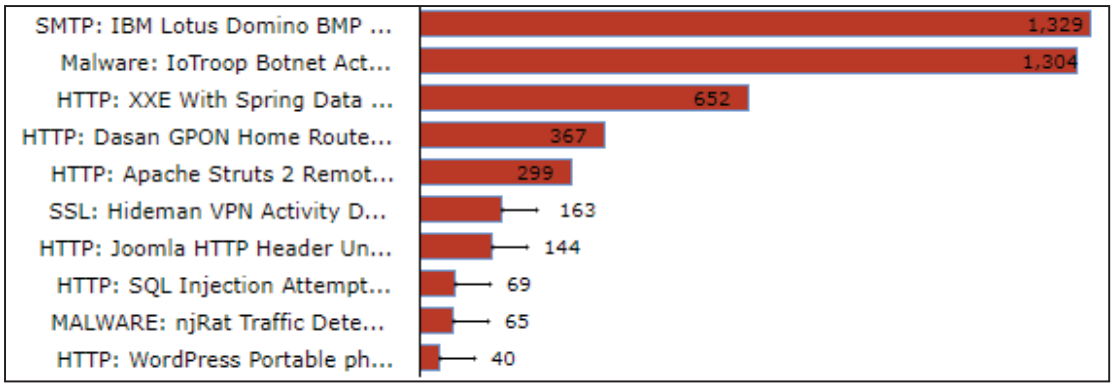


Figura N° 3: Se observa un total de 4.432 eventos detectados y mitigados por la herramienta IPS durante el mes de abril.

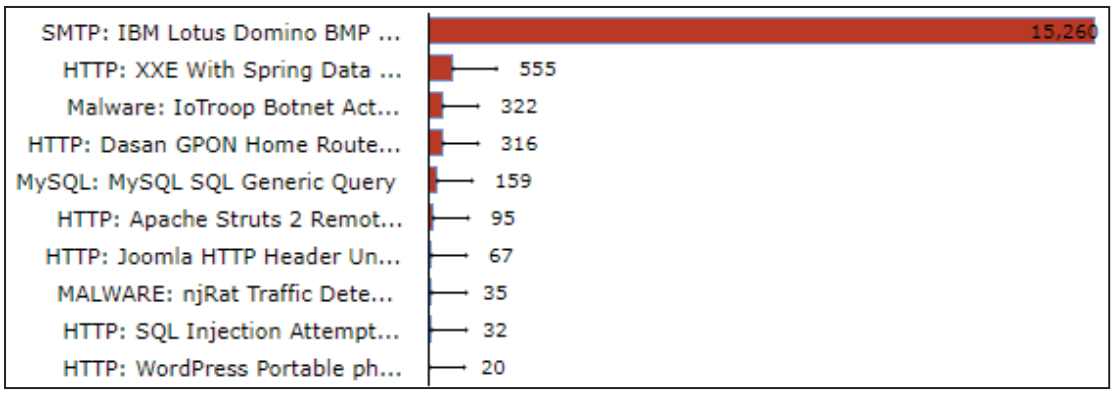


Figura N° 4: Se observa un total de 16.861 eventos detectados y mitigados por la herramienta IPS durante el mes de mayo.

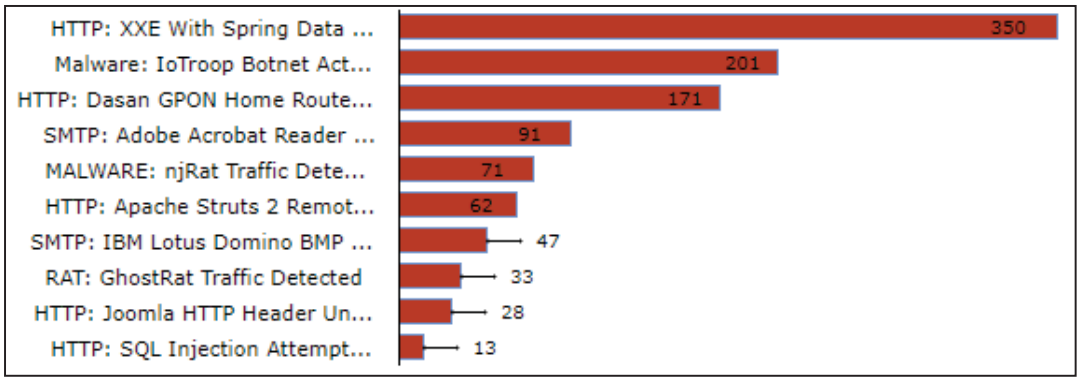


Figura N° 5: Se observa un total de 1.067 eventos detectados y mitigados por la herramienta IPS durante el mes de junio.

- Monitoreo Antimalware y antispam Office 365:

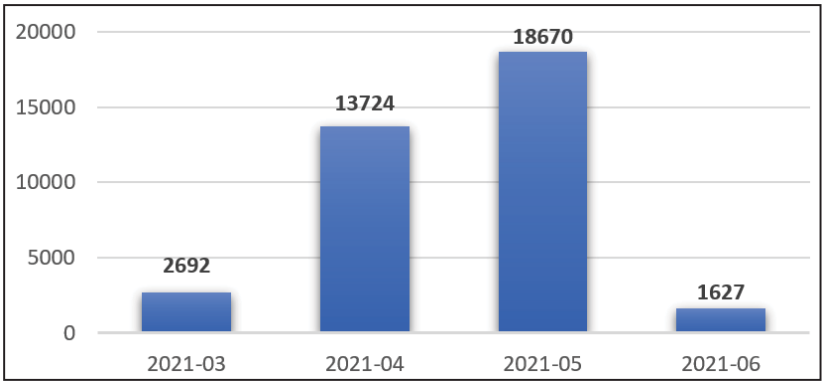
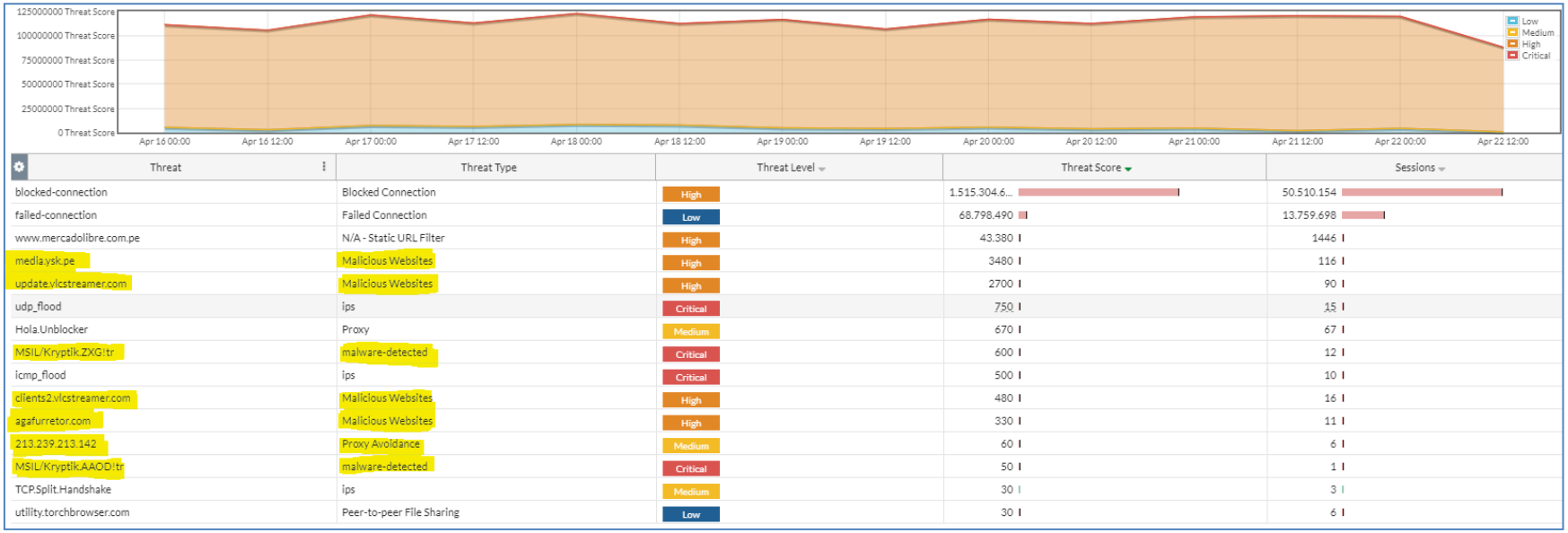


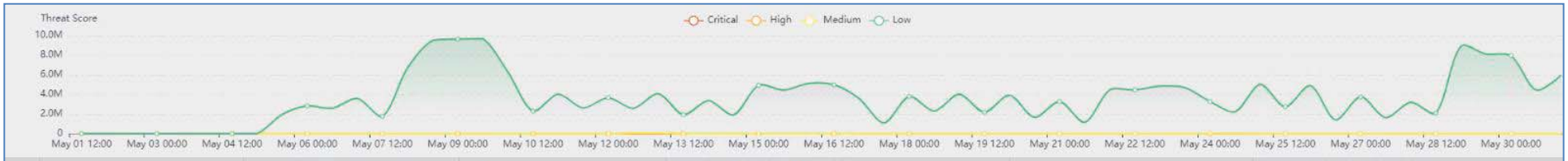
Figura N° 6: Se observa un total de 36.413 eventos detectados y mitigados por la herramienta antispam y antimalware de Office 365 entre marzo y junio del presente año.

- Herramienta Firewall Perimetral



Threat	Threat Type	Threat Level	Threat Score	Sessions
blocked-connection	Blocked Connection	High	1.515.304.6...	50.510.154
failed-connection	Failed Connection	Low	68.798.490	13.759.698
www.mercadolibre.com.pe	N/A - Static URL Filter	High	43.380	1446
medla.ysk.pe	Malicious Websites	High	3480	116
update.vlcstreamer.com	Malicious Websites	High	2700	90
udp_flood	ips	Critical	750	15
Hola.Unblocker	Proxy	Medium	670	67
MSIL/Kryptik.ZXG!tr	malware-detected	Critical	600	12
icmp_flood	ips	Critical	500	10
clients2.vlcstreamer.com	Malicious Websites	High	480	16
agafurretor.com	Malicious Websites	High	330	11
213.239.213.142	Proxy Avoidance	Medium	60	6
MSIL/Kryptik.AAOD!tr	malware-detected	Critical	50	1
TCP.Split.Handshake	ips	Medium	30	3
utility.torchbrowser.com	Peer-to-peer File Sharing	Low	30	6

Figura N° 7: Se observa un total de 1,799 eventos detectados y mitigados por la herramienta firewall perimetral durante el mes de abril.



#	Threat	Category	CVE ID	Threat Score(Blocked/ Allowed)	▼ Threat Level	Incidents(Blocked/ Allowed)
1	udp_flood	IPS		19,250	Critical	385
2	ip_dst_session	IPS		1,000	Critical	20
3	tcp_port_scan	IPS		550	Critical	11
4	ip_src_session	IPS		450	Critical	9
5	icmp_flood	IPS		250	Critical	5
6	tcp_src_session	IPS		200	Critical	4
7	udp_dst_session	IPS		150	Critical	3
8	W32/Delf.DCB!tr	Malware		100	Critical	2
9	tcp_syn_flood	IPS		50	Critical	1
10	media[dot]ysk[dot]pe	Malicious Websites		3,390	High	113
11	www.mercadolibre.com.pe	N/A - Static URL Filter		2,730	High	91
12	serch07[dot]biz	Malicious Websites		570	High	19
13	stats[dot]urban-vpn[dot]com	Proxy Avoidance		163,810	Medium	16,381
14	213[dot]239[dot]213[dot]142	Proxy Avoidance		2,220	Medium	222
15	Hola.Unblocker	Proxy		1,520	Medium	152
16	Atlassian.Jira.Authenticated.Upload.Remo	IPS		70	Medium	7
17	TCP.Split.Handshake	IPS		10	Medium	1

Figura N° 8: Se observa un total de 17,226 eventos detectados y mitigados por la herramienta firewall perimetral durante el mes de mayo.

#	Threat	Category	CVE ID	Threat Score(Blocked/ Allowed)	▼Threat Level	Incidents(Block
1	ip_dst_session	IPS		218,850	Critical	4,377
2	udp_dst_session	IPS		2,300	Critical	46
3	HTML/Agent.E3F2!tr	Malware		1,950	Critical	39
4	ip_src_session	IPS		1,150	Critical	23
5	tcp_src_session	IPS		700	Critical	14
6	tcp_syn_flood	IPS		700	Critical	14
7	tcp_port_scan	IPS		700	Critical	14
8	tcp_dst_session	IPS		700	Critical	14
9	W32/GenKryptik.DPIE!tr	Malware		250	Critical	5
10	udp_flood	IPS		250	Critical	5
11	HTML/Phishing.BTV!tr	Malware		100	Critical	2
12	MSIL/Kryptik.ABNE!tr	Malware		50	Critical	1
13	Malicious_Behavior.SB	Malware		50	Critical	1
14	media[dot]ysk[dot]pe	Malicious Websites		40,260	High	1,342
15	www.mercadolibre.com.pe	N/A - Static URL Filter		11,190	High	373
16	fajasmyd[dot]com	Phishing		4,590	High	153
17	HTTP.URI.SQL.Injection	IPS		2,940	High	98
18	cesarvallejocollege[dot]com	Phishing		2,880	High	96
19	agafurretor[dot]com	Malicious Websites		1,230	High	41
20	serch07[dot]biz	Malicious Websites		1,200	High	40
21	pdloader[dot]com	Malicious Websites		1,080	High	36
22	enel[dot]zyxmeapp[dot]com	Phishing		930	High	31
23	azoaltou[dot]com	Malicious Websites		840	High	28
24	querilis[dot]com	Malicious Websites		630	High	21
25	fkvdha[dot]com	Spam URLs		600	High	20
26	www[dot]flowsurfv3[dot]net	Malicious Websites		600	High	20
27	onemboaran[dot]com	Malicious Websites		540	High	18
28	denetsuk[dot]com	Malicious Websites		390	High	13
29	goajuzey[dot]com	Malicious Websites		360	High	12
30	thingsrefutation[dot]com	Spam URLs		360	High	12
31	genuinesubqueries[dot]com	Spam URLs		240	High	8
32	forzubatr[dot]com	Malicious Websites		180	High	6
33	y0utube[dot]services	Spam URLs		150	High	5
34	etrecantformation[dot]com	Spam URLs		150	High	5

Figura N° 9: Se observa un total de 6,933 eventos detectados y mitigados por la herramienta firewall perimetral durante el mes de junio.

- Anti-Denegación de Servicio

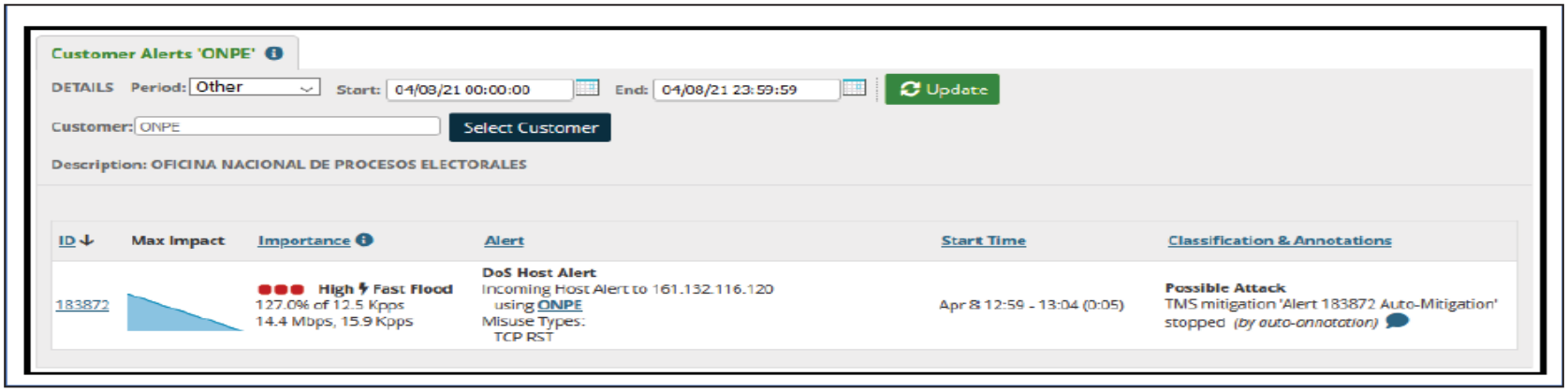


Figura N° 10: Se observa un evento detectado y mitigado por la herramienta anti DoS durante el mes de abril.

- Firewall de Aplicaciones Web (WAF) Cloud

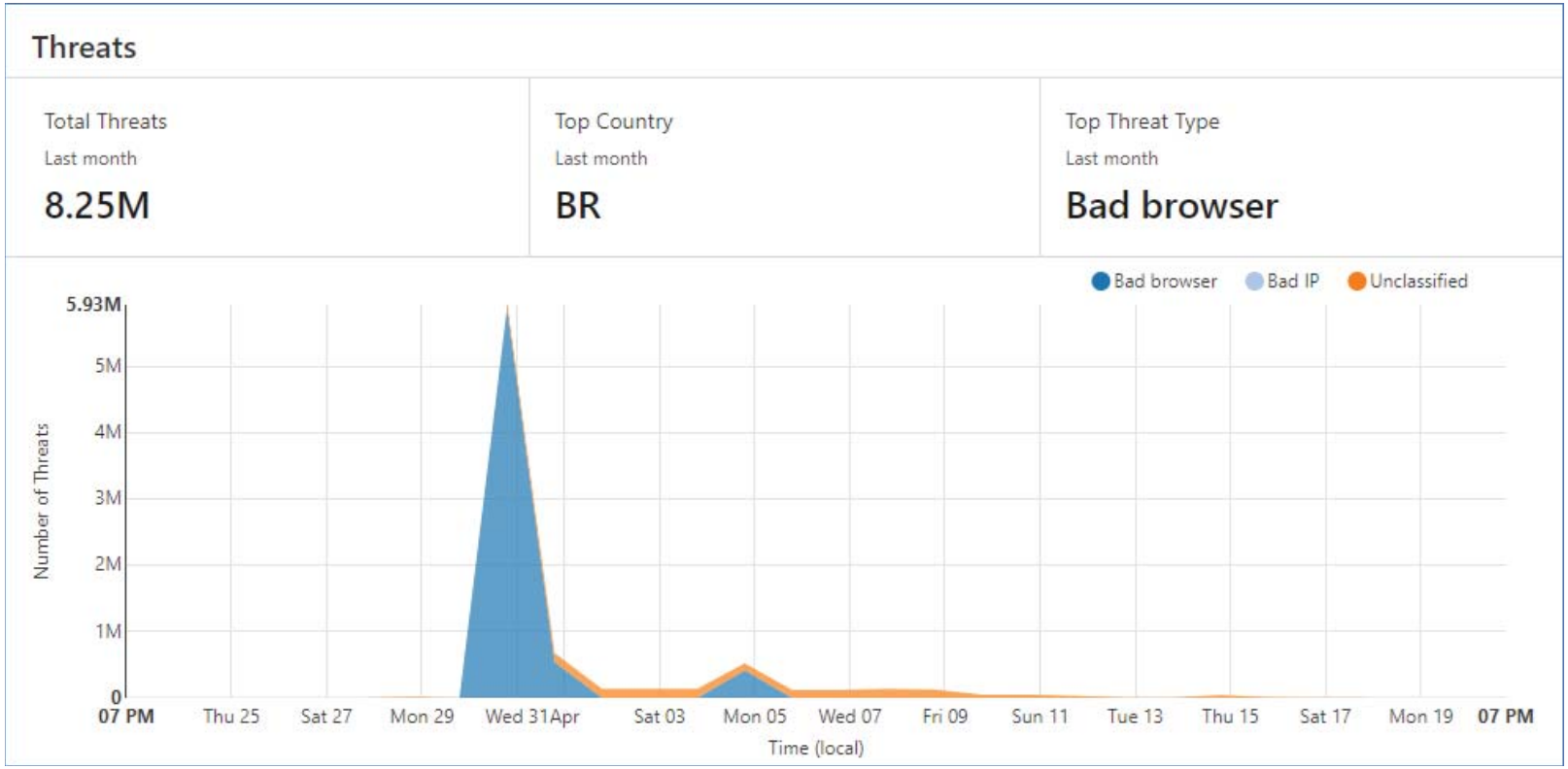


Figura N° 11: Se observa un total de 8.25 millones de eventos detectados y mitigados por la herramienta WAF para aplicaciones cloud durante el mes de abril.

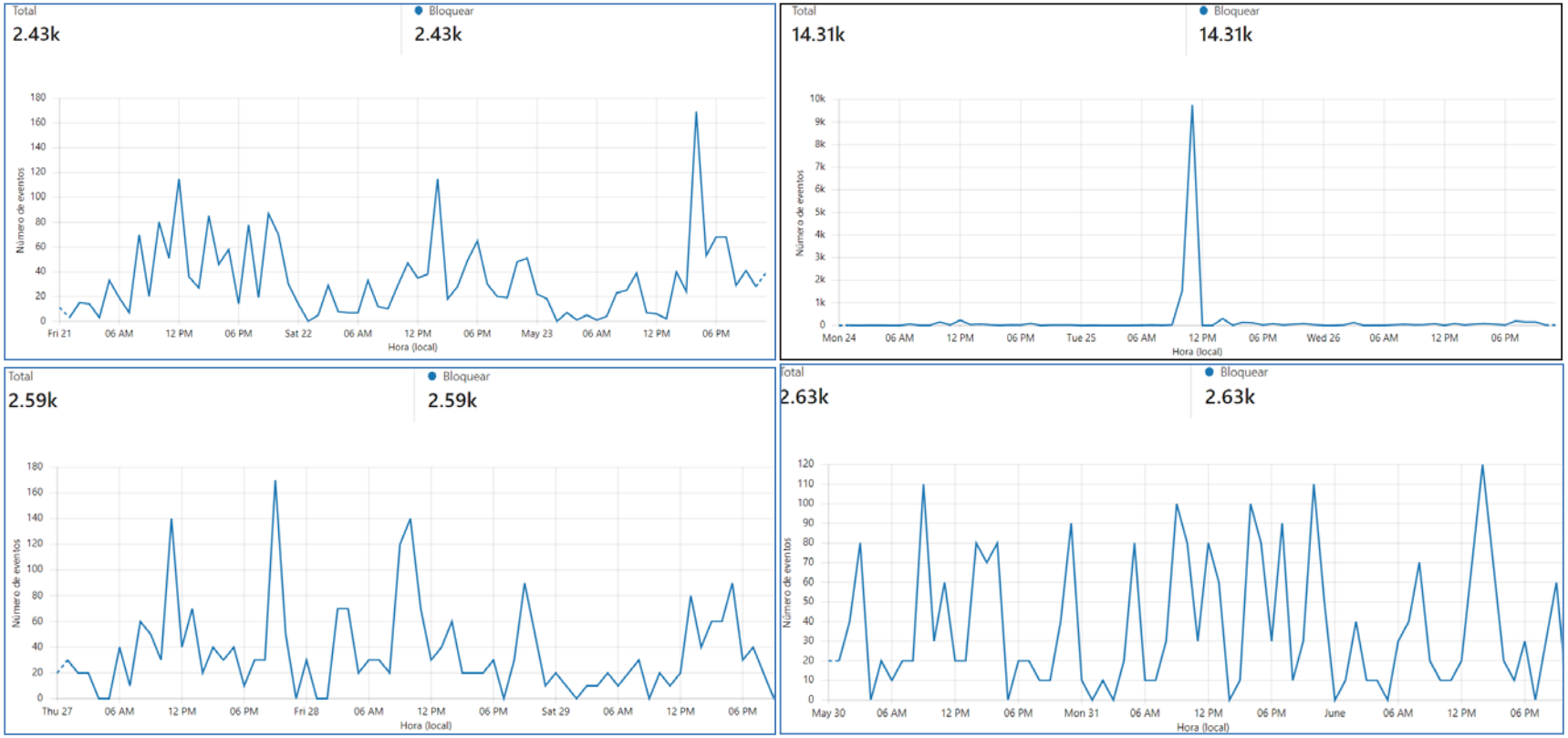


Figura N° 12: Se observa un total de 21.960 eventos detectados y mitigados por la herramienta WAF Cloud durante el mes de mayo.

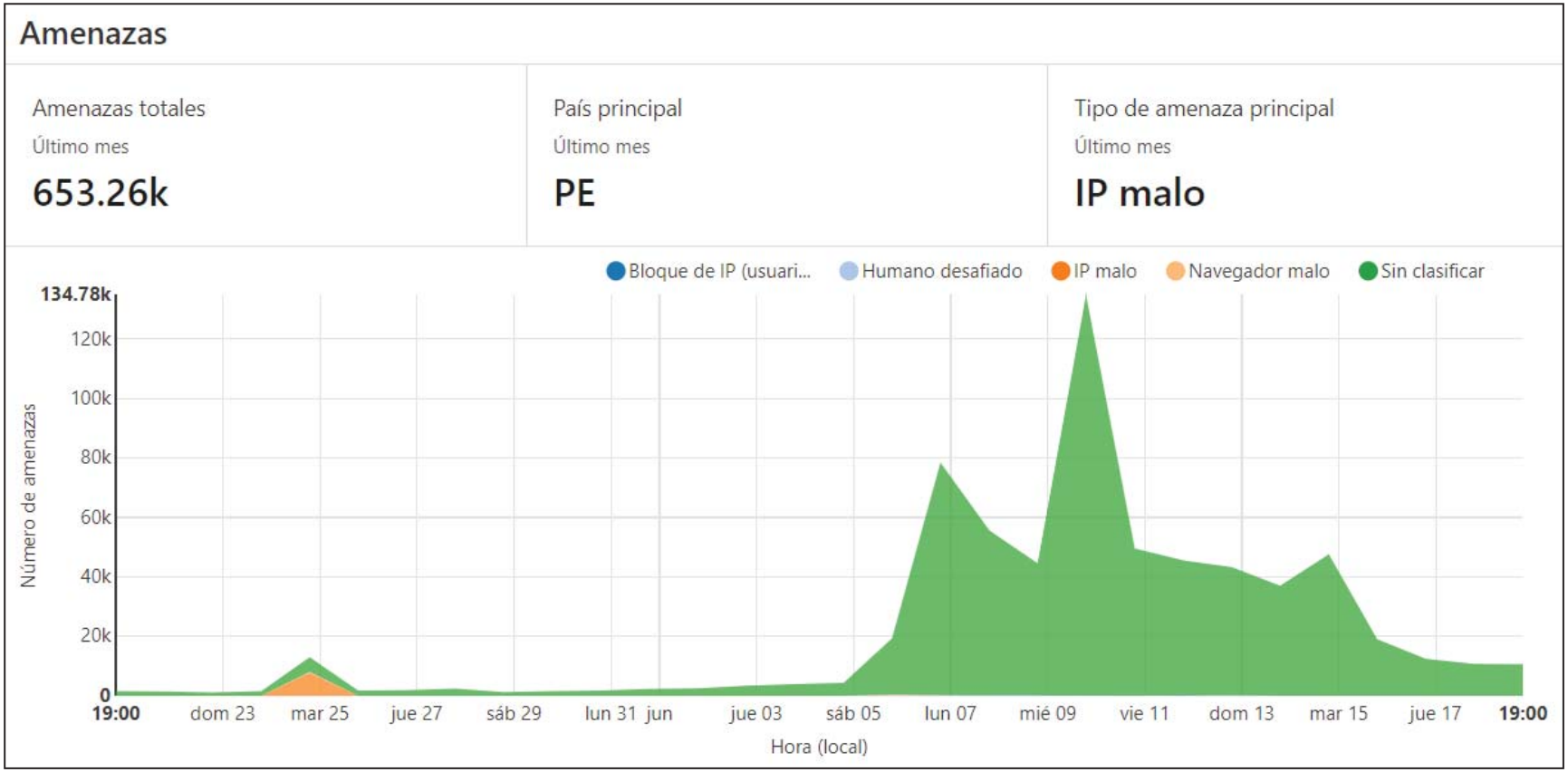


Figura N° 13: Se observa un total de 653.260 eventos detectados y mitigados por la herramienta WAF para aplicaciones cloud durante el mes de junio.

- WAF On premise

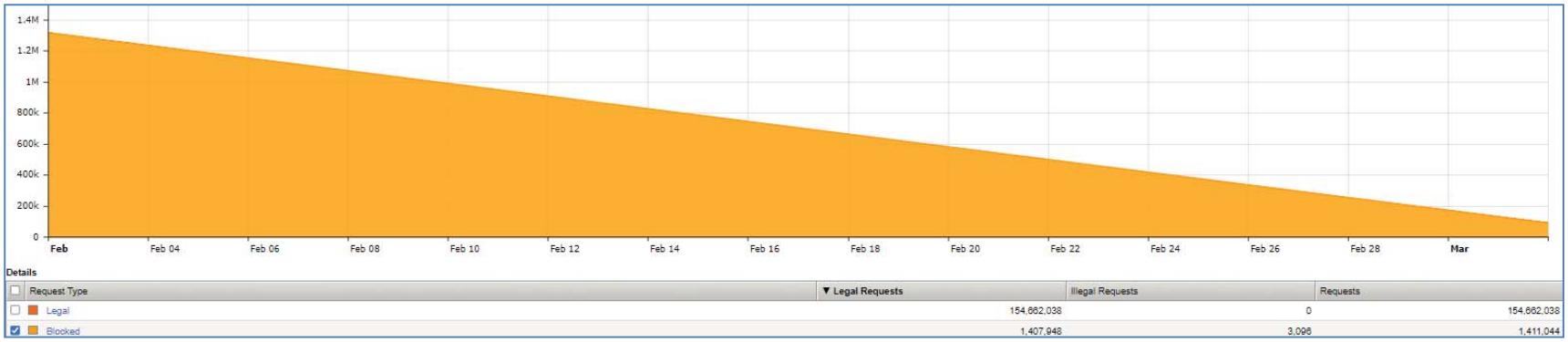


Figura N° 14: Se observa un total de 1.411.044 eventos detectados y mitigados por la herramienta WAF para aplicaciones on premise durante el mes de febrero.

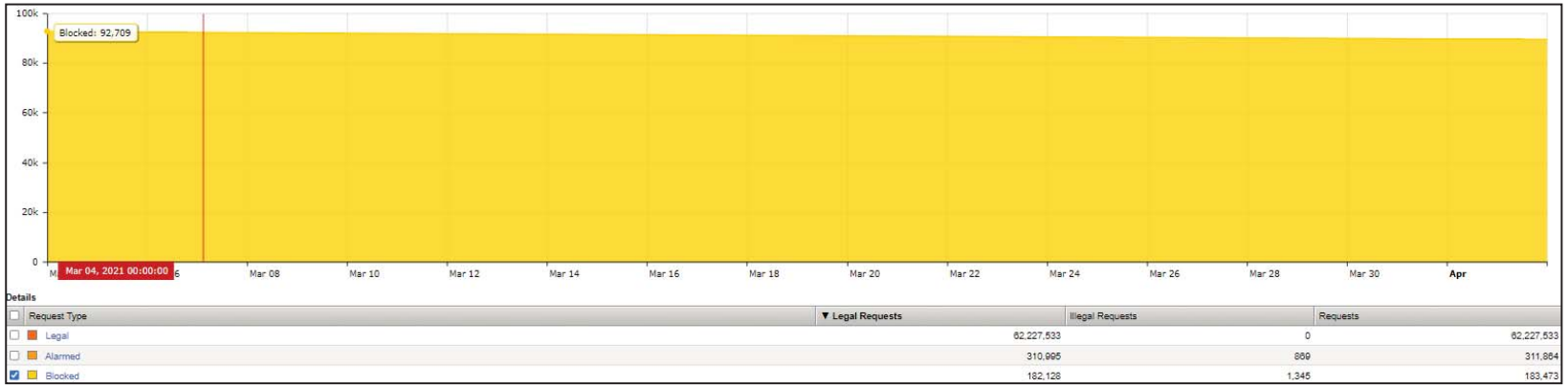


Figura N° 15: Se observa un total de 311.864 eventos detectados y mitigados por la herramienta WAF para aplicaciones on premise durante el mes de marzo.

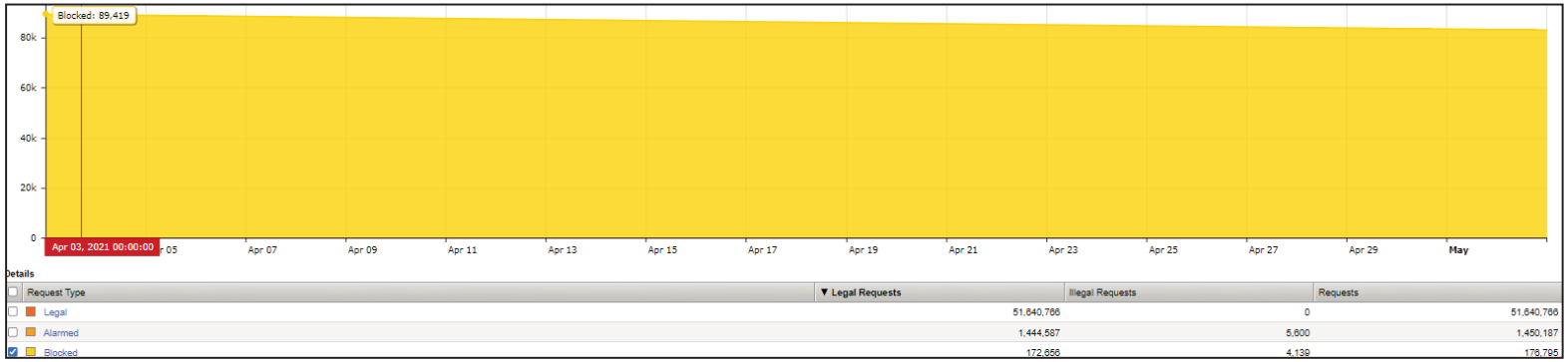


Figura N° 16: Se observa un total de 176.795 eventos detectados y mitigados por la herramienta WAF para aplicaciones on premise durante el mes de abril.

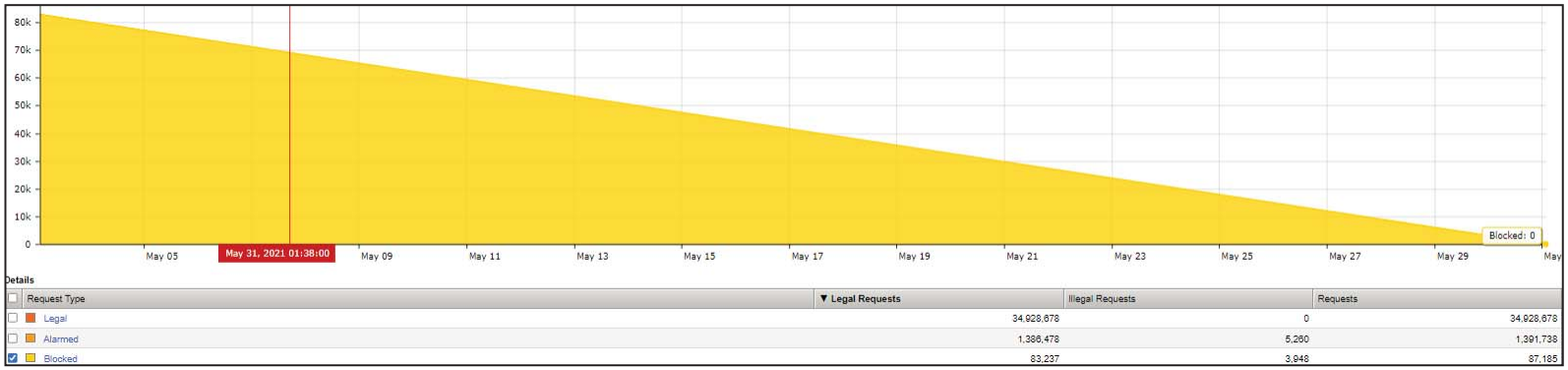
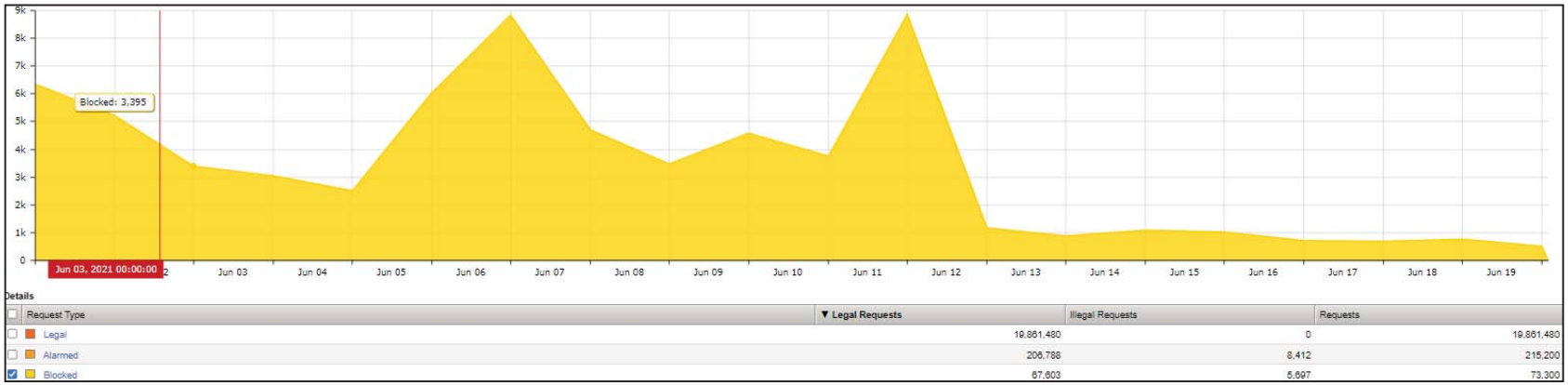


Figura N° 17: Se observa un total de 87.185 eventos detectados y mitigados por la herramienta WAF para aplicaciones on premise durante el mes de mayo.



Details

Request Type	▼ Legal Requests	Illegal Requests	Requests
Legal	19,861,480	0	19,861,480
Alarmed	206,788	8,412	215,200
Blocked	67,603	5,697	73,300

Figura N° 18: Se observa un total de 73.300 eventos detectados y mitigados por la herramienta WAF para aplicaciones on premise durante el mes de junio.

- Antimalware (Antivirus)

Acción	Virus	Spyware
Limpiado/bloqueado	1	0
Eliminado	20	5
En cuarentena	2	2
Sospechoso	0	0
Recientemente infectado	0	0
Aún infectado	0	0

Tabla N° 4: Se observa un total de 30 eventos detectados y mitigados por la herramienta antivirus durante el mes de mayo.

Acción	Virus	Spyware
Limpiado/bloqueado	1	2
Eliminado	12	8
En cuarentena	2	0
Sospechoso	0	0
Recientemente infectado	0	0
Aún infectado	0	0

Tabla N° 5: Se observa un total de 25 eventos detectados y mitigados por la herramienta antivirus durante el mes de junio.

Cabe mencionar que, durante las elecciones, las herramientas detectaron y mitigaron eventos de Ciberseguridad por lo que no se registraron incidentes que causen indisponibilidad o degradación de los servicios que dan soporte a las EG 2021.

Actividad 2: Gestionar servicios relacionados a Ciberseguridad.

Acciones realizadas:

Se supervisó la ejecución del servicio Ethical Hacking EG 2021. Tal como se evidencia en los siguientes informes:

Informe: 000033-2021-DRB-SGIST-GITE (10MAY2021), INFORME DE CONFORMIDAD POR EL ENTREGABLE 1 Y 2 DEL SERVICIO DE ETHICAL HACKING – EG 2021.

Informe: 000029-2021-DRB-SGIST-GITE (19MAR2021), INFORME DE CONFORMIDAD POR EL ENTREGABLE 1 DEL SERVICIO DE ETHICAL HACKING – EG 2021.

Informe: 000027-2021-DRB-SGIST-GITE (17MAR2021), ATENDER | MPVE - REMITE SOLICITUD PARA INCREMENTAR UN PERSONAL ADICIONAL REFEERNCIA SERVICIO ETHICAL HACKING EG 2021.

Informe: 000026-2021-DRB-SGIST-GITE (26FEB2021), En el marco del Servicio Ethical Hacking EG 2021, se verifica que las propuestas de los postores Kunak Consulting S.A.C. y Strategos y Asociados S.A.C. se encuentran conforme a lo indicado en el TDR.

Informe: 000023-2021-DRB-SGIST-GITE (19FEB2021), Se remite pliego de consultas con respuestas y TDR modificado del SERVICIO DE ETHICAL HACKING – EG 2021.

Informe: 000010-2021-DRB-SGIST-GITE (22ENE2021), Se remite formato de cumplimiento FM07 revisado sin Observación para la contratación del servicio de Ethical Hacking 2021 ATENDER | Revisado sin Observación / Formato FM07-GAD/LOG para la contratación del "SERVICIO DE ETHICAL HACKING - EG 2021" SE REMITE FORMATO DE CUMPLIMIENTO FM07 A SGOI PARA REVISIÓN

Actividad 3: Coordinar reuniones semanales con los integrantes del CSIRT Electoral.

Acciones realizadas:

Con el Informe N° 000017-2020-DRB-SGIST-GITE 03NOV2020 se solicitó a la SGIST su gestión para que la GITE propicie la reactivación del Equipo de Respuesta a Incidentes de Seguridad Digital CSIRT. La gestión de la SGIST se realizó con Informe N° 001428-2020/SGIST-GITE 31DIC2020.

A su vez, la GITE emitió el MEMORANDO N° 003779-2020-GITE/ONPE 31DIC2020 con el que solicita a la Secretaría General hacer de conocimiento al Director de Registros, Estadística y Desarrollo Tecnológico del Jurado Nacional de Elecciones (Ing. Luis Alberto Antonio Ramos Llanos) y a la Gerente de Tecnología de la Información del Registro Nacional de Identificación y Estado Civil (Rosario Roxana Dávila Olórtegui) la reactivación del CSIRT Electoral en el marco de las EG2021.

Finalmente, la Secretaría General emitió los siguientes oficios comunicando a las entidades la reactivación del CSIRT Electoral:

- OFICIO N° 000018-2021/SG 06ENE2021 dirigido al Ministerio de Defensa.
- OFICIO N° 000019-2021/SG 06ENE2021 dirigido al JNE.
- OFICIO N° 000020-2021/SG 06ENE2021 dirigido al RENIEC.

Como resultado de las coordinaciones realizadas, el 12ENE2021 se realizó la reunión de reinicio de las actividades del CSIRT Electoral. URL del video https://web.microsoftstream.com/video/a771200f-306b-44e3-861e-b02936c1a60c

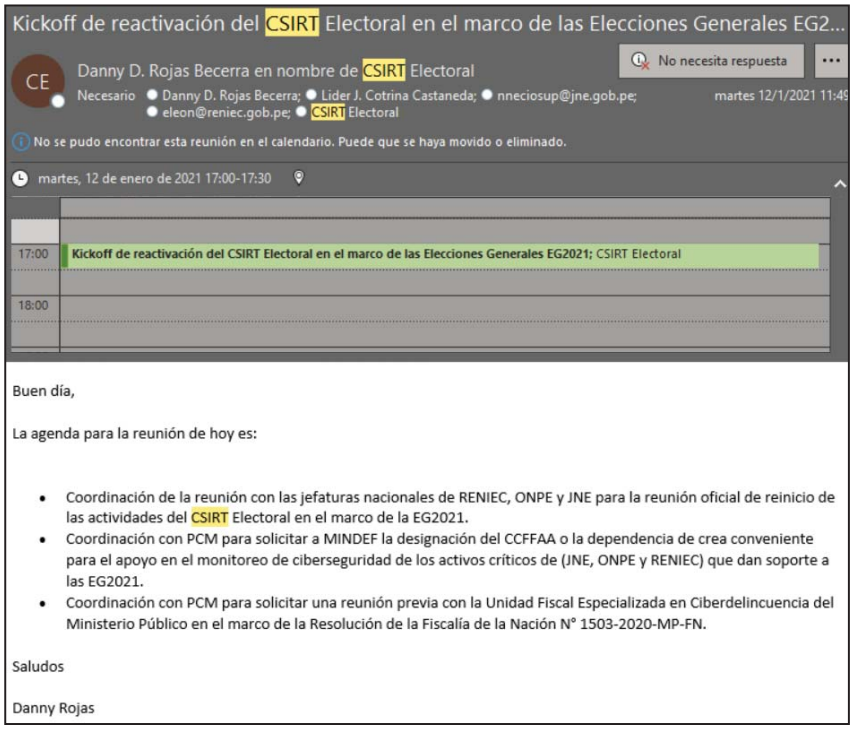


Figura N° 19: Agenda de la reunión de reinicio de actividades del CSIRT Electoral 12ENE2021

Actividades realizadas en febrero:

Apertura del Grupo oficial de comunicación en Telegram:

Figura N° 20: Grupo de Telegram para coordinación de incidentes 10FEB2021

Figura N° 21: Reunión de coordinación de plan de acción de incidentes realizada el 11FEB2021

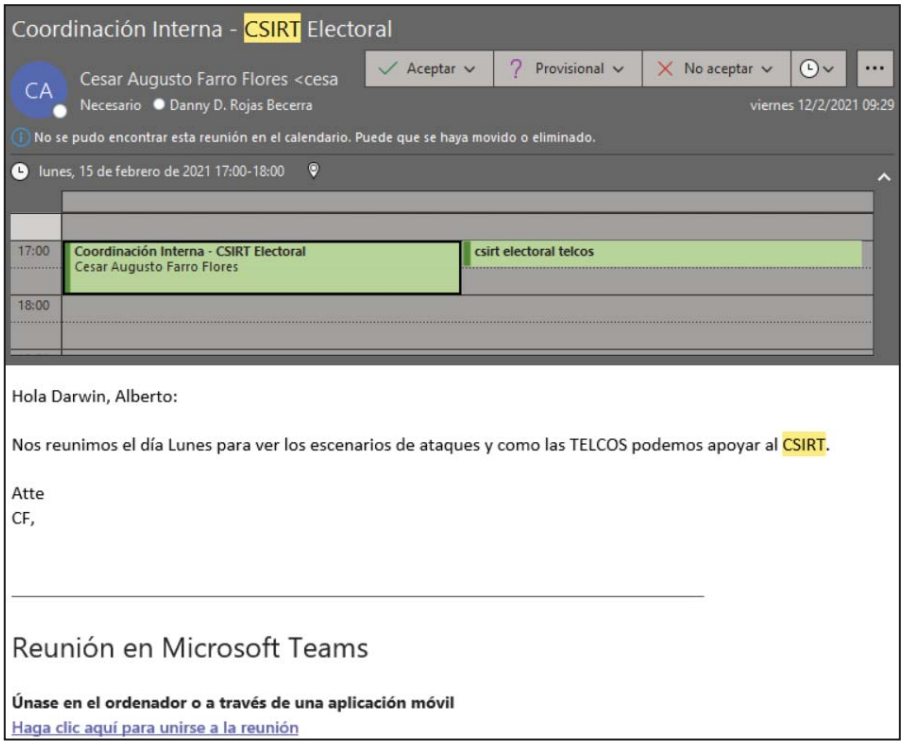


Figura N° 22: Continuación de la reunión de coordinación de plan de acción de incidentes realizada el 13FEB2021

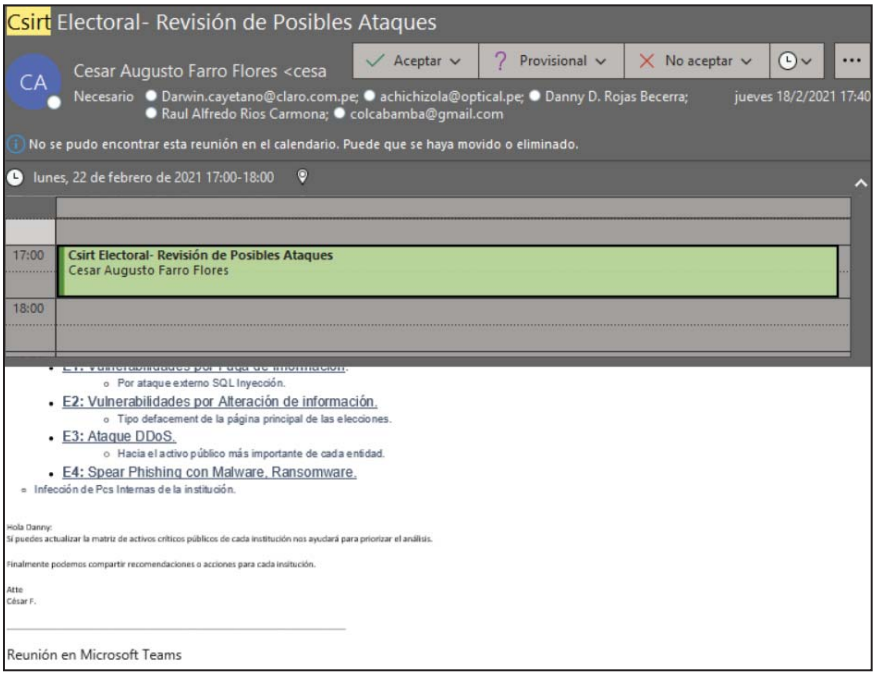


Figura N° 23: Reunión de coordinación realizada el 22FEB2021 con especialistas de las entidades y los proveedores ISP.

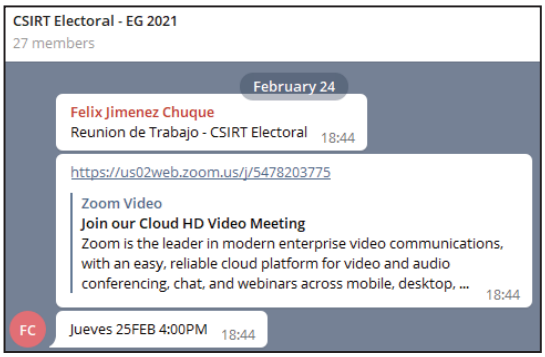


Figura N° 24: Reunión de coordinación general realizada el 25FEB2021 para la gestión de incidentes ejecutada por los proveedores ISP.

Actividades efectuadas en marzo:

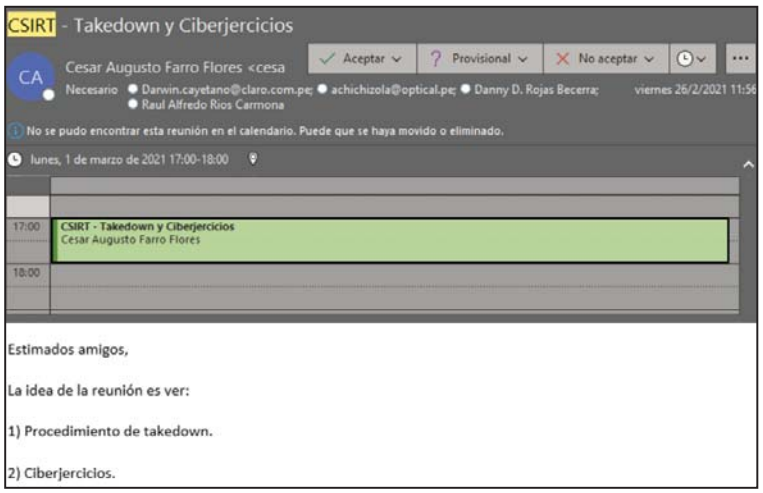


Figura N° 25: Reunión realizada el 01MAR2021 con especialistas de las entidades y los proveedores ISP para planificar de Ciberejercicios.

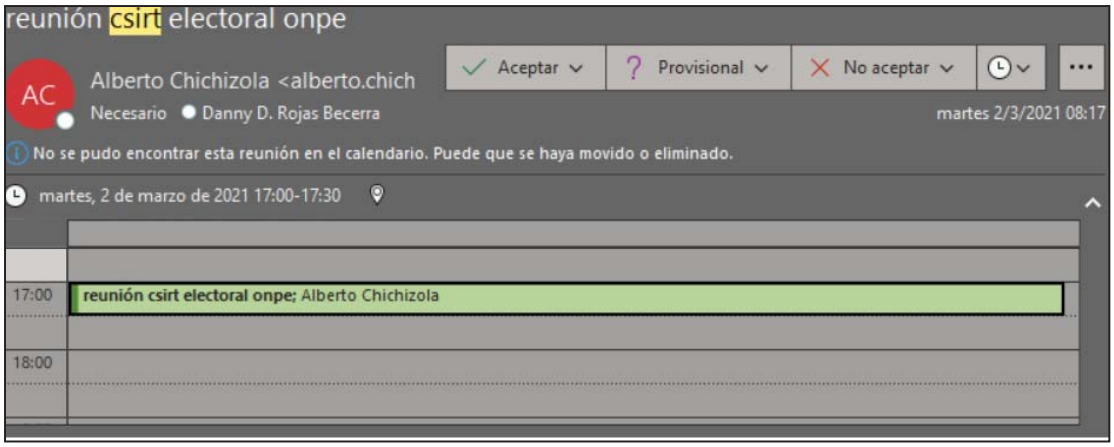


Figura N° 26: Reunión de coordinación 1:1 realizada el 02MAR2021 para analizar la gestión de incidentes de Ciberseguridad en cada entidad.

Figura N° 27: Reunión de coordinación general realizada el 04MAR2021, para dar a conocer las Ciberamenazas durante elecciones.

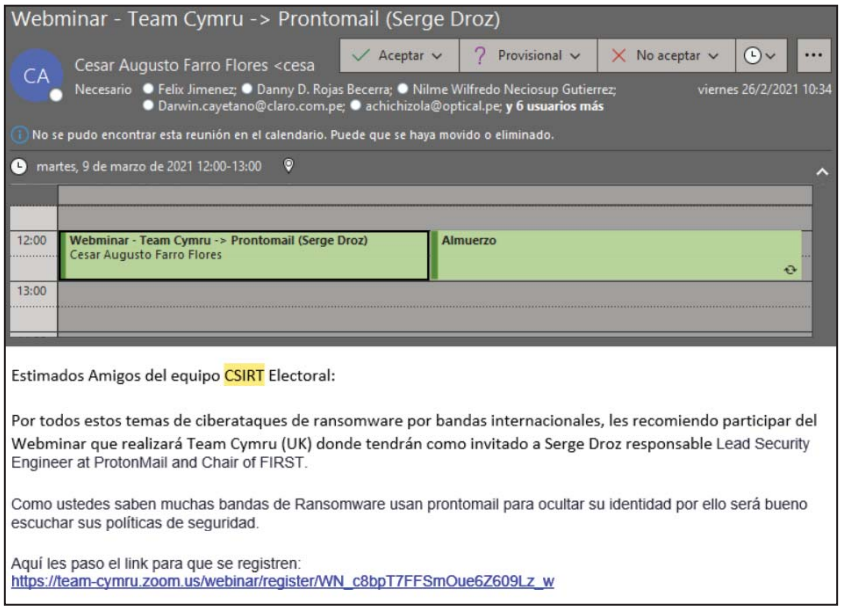


Figura N° 28: Reunión realizada el 09MAR2021, para presentar la metodología del CSIRT.

Figura N° 29: Reunión realizada el 25MAR2021, para presentar la matriz de contactos.

Actividades efectuadas en abril:

Figura N° 30: Reunión realizada el 01ABR2021, para elaborar la matriz de activos críticos.

Actividades efectuadas en mayo:

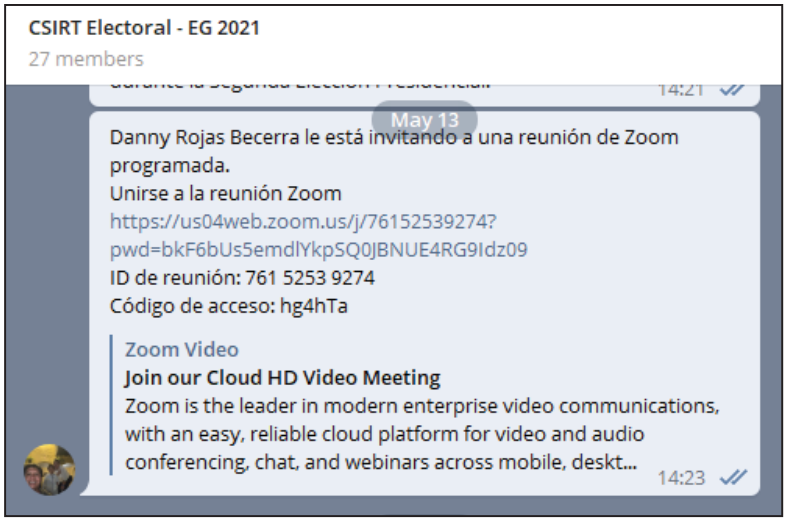


Figura N° 31: Reunión de coordinación general realizada el 13MAY2021, donde se indicaron procedimientos de mitigación de software malicioso.

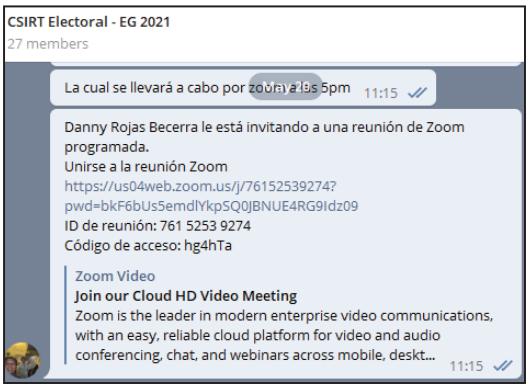


Figura N° 32: Reunión de coordinación general realizada el 20MAY2021, donde se indicaron los tipos de ataques que provocan una posible denegación de servicio de los sistemas web publicados en Internet.

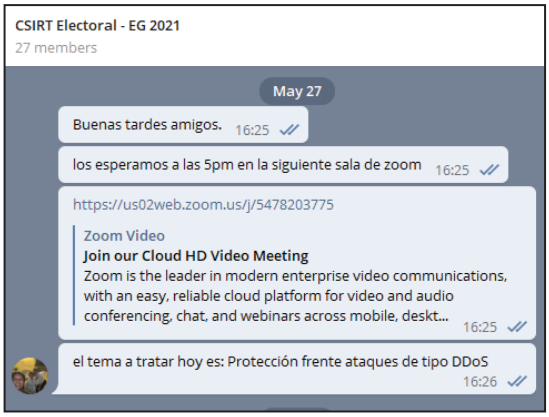


Figura N° 33: Reunión de coordinación general realizada el 27MAY2021, donde se aclararon los contactos de escalamiento en caso ocurra un incidente de Ciberseguridad.

Actividades efectuadas en junio:

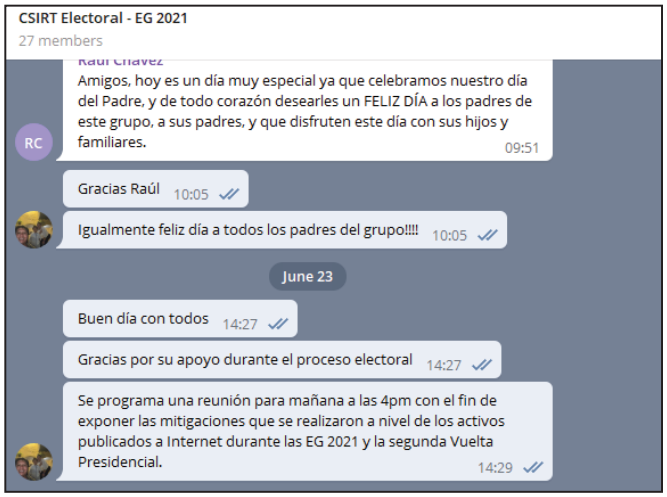


Figura N° 34: Reunión de coordinación general realizada en 23JUN2021 donde se mostraron los resultados de las mitigaciones realizadas durante el día de elección.

Actividad 4: Realizar el seguimiento al monitoreo efectuado por los integrantes del CSIRT Electoral.

Acciones realizadas:

Por medio del Telegram oficial se efectuó el seguimiento al monitoreo efectuado por los integrantes del CSIRT Electoral con el fin de proponer medidas de mitigación y respuesta.

El monitoreo consiste en verificar la disponibilidad e integridad de los servicios publicados hacia internet como son:

- ✓ SEA (Sistema de Escrutinio Automatizado)
- ✓ Web de Resultados
- ✓ Web institucional
- ✓ SIDE (Sistema de Información del Día de Elección)
- ✓ ONPEDUCA
- ✓ CLV (Consulta tu Local de Votación)
- ✓ Elige tu local de votación
- ✓ Consulta miembro de mesa

El monitoreo efectuado por los integrantes del CSIRT Electoral, permite tener una cobertura de observación durante 24 horas, durante los 7 días de la semana, para detectar cualquier incidente que ocurra en los portales web publicados a Internet.

Alertas realizadas en febrero:

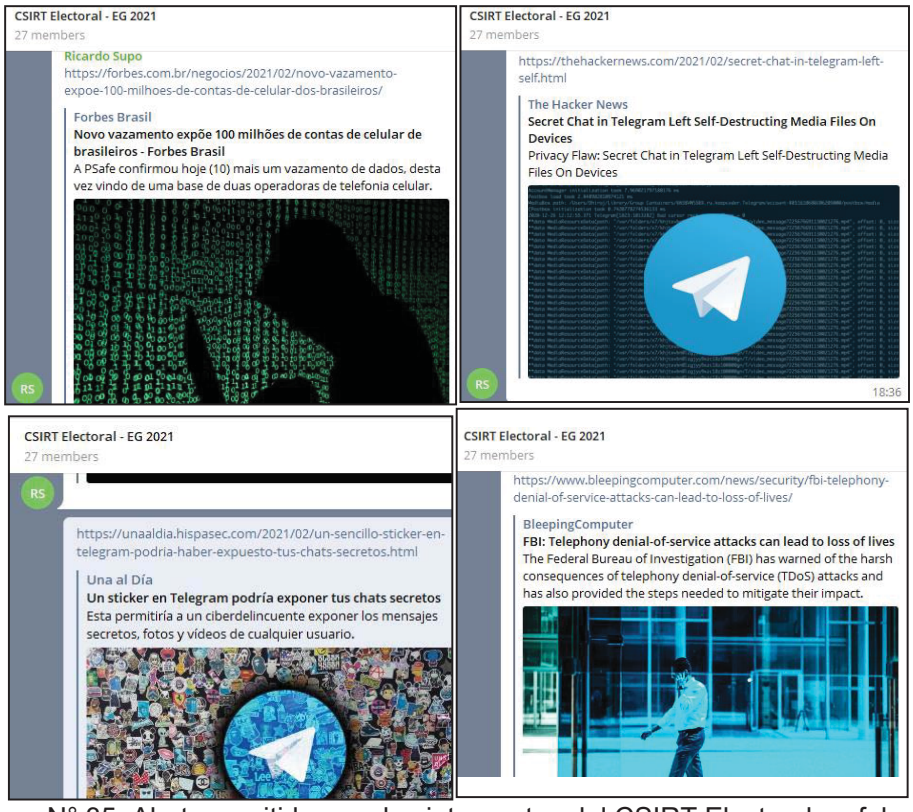


Figura N° 35: Alertas emitidas por los integrantes del CSIRT Electoral en febrero.

Alertas realizadas en marzo:

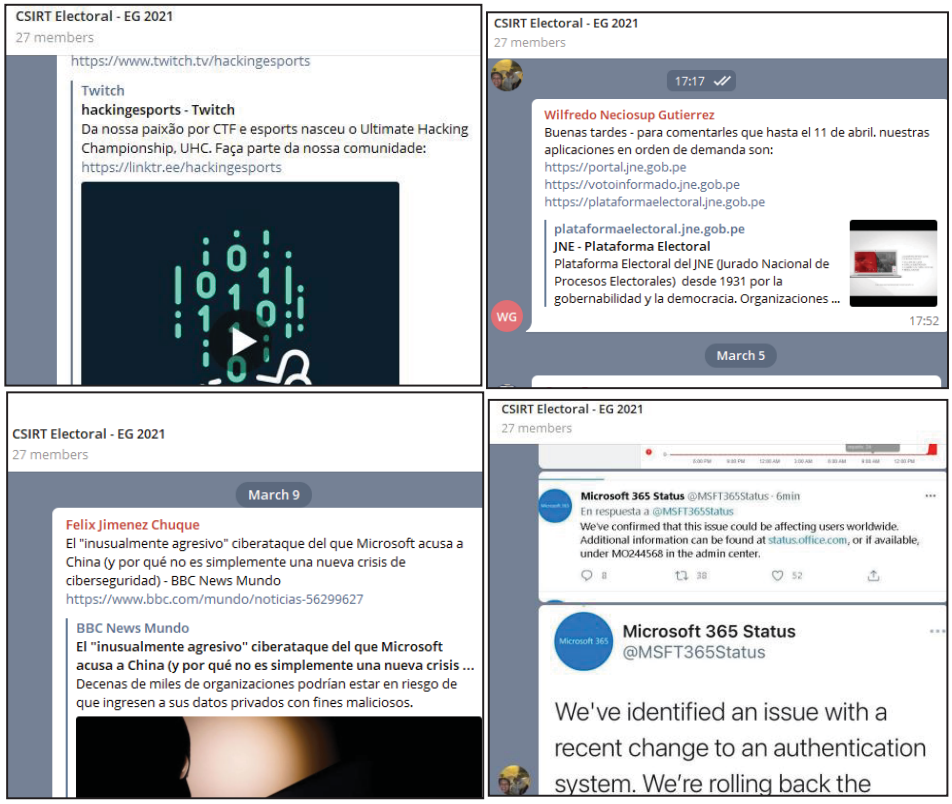


Figura N° 36: Alertas emitidas por los integrantes del CSIRT Electoral en marzo.

Alertas realizadas en abril:

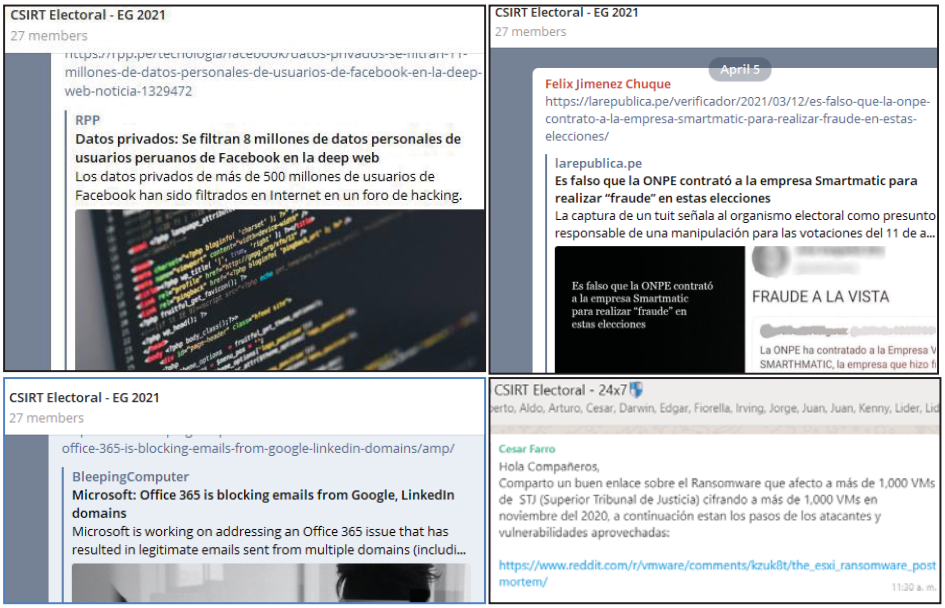


Figura N° 37: Alertas emitidas por los integrantes del CSIRT Electoral en abril.

Alertas realizadas en mayo:

Figura N° 38: Se detectaron 04 eventos relacionados a ciberataque a gobierno extranjero, campaña de phishing, campaña de malware y Vulnerabilidad en sistemas virtuales.

Alertas realizadas en junio:

Figura N° 39: Se detectaron 04 eventos relacionados a mensaje falso respecto a elecciones, amenazas de ataque a entidades del gobierno peruano, fuga masiva de información y difusión de noticias maliciosas.

2.2 Reporte del Indicador del Plan de Ciberseguridad para la EG 2021

Con respecto al objetivo de lo programado:

- Evitar incidentes a los activos informáticos que dan soporte a la EG2021.

Se aprecia el siguiente resultado en el indicador:

Indicador 1: Porcentaje de eventos de Ciberseguridad bloqueados.

$$\left[\frac{X*100\%}{X+Y}\right] = \left[\frac{11{,}079{,}731*100\%}{11{,}079{,}731+0}\right]$$

Meta = 98% **Resultado** = 100%

X = Número de eventos de Ciberseguridad bloqueados = 11,079,731
Y = Número de Incidentes que afectaron los activos de información y servicios informáticos = 0

Corresponde señalar que, durante el día de la Jornada Electoral, todos los eventos de Ciberseguridad fueron bloqueados y no se registraron incidentes que afectaron a los activos de información y servicios informáticos.

III. BALANCE GENERAL

3.1. Logros Obtenidos

- Se ejecutaron el 136% de las tareas programadas en el Plan de Ciberseguridad para la EG 2021, tal como se muestra a continuación:

Tareas	Cantidad
Programadas	14
Ejecutadas	19

Tabla N° 6: Tareas

- Durante los meses de febrero a junio se logró bloquear 11,079,731 eventos adversos los mismos que no registraron incidentes ni afectación a los activos de información y servicios informáticos.

3.2. Problemas identificados y medidas correctivas adoptadas

No se presentaron inconvenientes durante la ejecución del Plan de Ciberseguridad.

IV. EJECUCIÓN DEL PRESUPUESTO

En las actividades establecidas en el Plan de Ciberseguridad para la EG 2021 se ejecutó un primer monto con valor estimado de S/. 26.000.00. Dicho cálculo se obtuvo considerando el pago mensual del personal asignado como “Servicio de Locador de servicio de Especialista de Ciberseguridad”:

#	DESCRIPCIÓN ITEMS – PROGRAMADOS	RETRIBUCIÓN MENSUAL	FECHA DE INICIO DE ACTIVIDADES	PRESUPUESTO PROYECTADO 1ERA - VUELTA				
				TOTAL ENERO	TOTAL FEBRERO	TOTAL MARZO	TOTAL ABRIL	TOTAL
1	ESPECIALISTA DE CIBERSEGURIDAD	6,500.00	07/01/2021	6,500.00	6,500.00	6,500.00	6,500.00	26,000.00

Tabla N° 7: Ejecución del presupuesto conforme a lo indicado por SGOI

V. CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

- Todos los eventos detectados por las herramientas de Ciberseguridad fueron mitigados.
- No ocurrieron incidentes de Ciberseguridad en los activos informáticos que dieron soporte a la EG2021.
- Se mitigó un total de 11,079,731 eventos de Ciberseguridad tal como se muestran en la Tabla N° 3.

Recomendaciones:

Se recomienda continuar con el monitoreo permanente de los eventos de Ciberseguridad con la finalidad de preservar la confidencialidad, disponibilidad e Integridad de la Información de la entidad.