OFICINA NACIONAL DE PROCESOS ELECTORALES

INFORME DE EVALUACIÓN

PLAN DE CIBERSEGURIDAD PARA LAS EMC 2021

Elaborado por:

Gerencia de Informática y Tecnología Electoral

ONPE Firma Digital
OFICINA NACIONAL DE PROCESOS ELECTORALES
Firmado digitalmente por SAMAME BLAS Jose Edilberto FAU 20291973851 soft
Motivo: Doy V° B°
Fecha: 21.12.2021 16:21:56 -05:00

ONPE Firma Digital
OFICINA NACIONAL DE PROCESOS ELECTORALES
Firmado digitalmente por MONTENEGRO VEGA Roberto Carlos FAU 20291973851 soft
Motivo: Doy V° B°
Fecha: 22.12.2021 22:31:29 -05:00

LIMA, DICIEMBRE 2021

INDICE

ABREVIATURAS

Elecciones Municipales Complementarias 2021	EMC 2021
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

I. RESUMEN EJECUTIVO

La finalidad del presente informe es evaluar lo establecido en el "Plan de Ciberseguridad para las Elecciones Municipales Complementarias 2021" aprobado con Resolución Gerencial N° 000010-2021-GITE/ONPE, en adelante denominado **PLAN**.

La evaluación consiste en verificar el cumplimiento de su objetivo, el cual está alineado a fortalecer la organización de los procesos electorales para la población electoral, por medio de asegurar los sistemas informáticos de la entidad y asegurar la información generada en el marco de las Elecciones Municipales Complementarias 2021.

Con relación al cumplimiento del objetivo descrito en el PLAN, es preciso indicar que, durante las elecciones, las herramientas detectaron y mitigaron todos los eventos de Ciberseguridad por lo que no se registraron incidentes que causen indisponibilidad o degradación de los servicios que dan soporte a las EMC 2021.

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

2.1 Descripción de acciones

A continuación, se detallan las acciones realizadas por cada actividad indicada en el FM11-GPP/PLAN: Evaluación de Planes especializados Acción.

Acción 1: Monitorear las herramientas de Ciberseguridad.

Durante los meses de septiembre y octubre, con ayuda de las herramientas de ciberseguridad, se llevó a cabo el monitoreo de las aplicaciones electorales publicadas en Internet, lo que permitió la detección de eventos en seguridad, así como aplicar el tratamiento correspondiente para su mitigación en forma oportuna, siendo posible garantizar la disponibilidad e integridad de las referidas aplicaciones.
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:

Herramienta	Septiembre	Octubre	Suma de eventos
Sistema de prevención de Intrusos (IPS)	21,049	1,590	22,639
Monitoreo Antimalware y antispam Office 365	41,566	33,710	75,276
Firewall Perimetral	2,490	175,189,964	175,192,454
Anti-Denegación de Servicio	0	0	0
Firewall de Aplicaciones Web Cloud	0	0	0
Firewall de Aplicaciones Web On premise	6,291,453	3,095,962	9,387,415
Antimalware (Antivirus)	94	22	116
		TOTAL	184,677,900

Tabla 1: Total de 184,677,900 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):

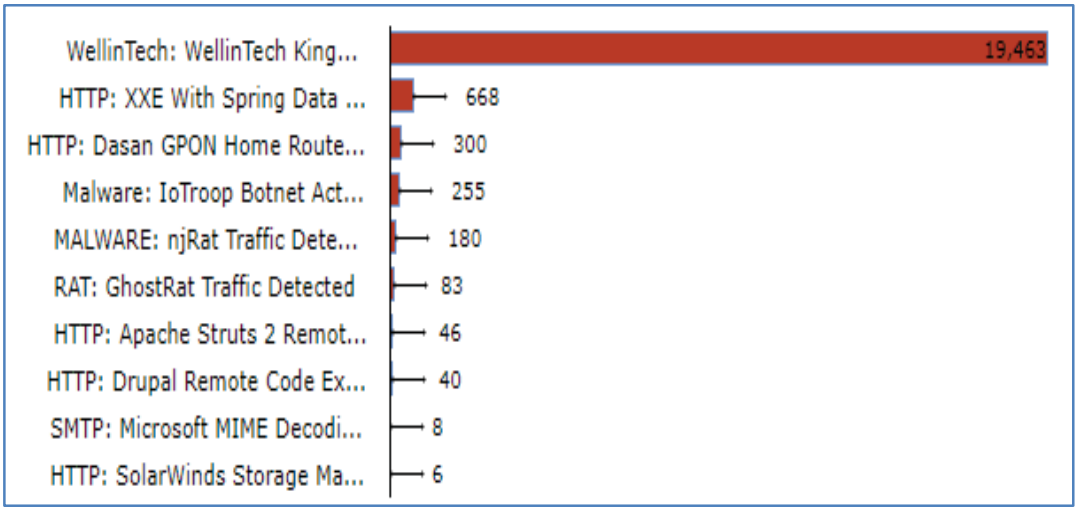


Figura N° 1: Se observa un total de 21,049 eventos detectados y mitigados por la herramienta IPS durante el mes de Septiembre.

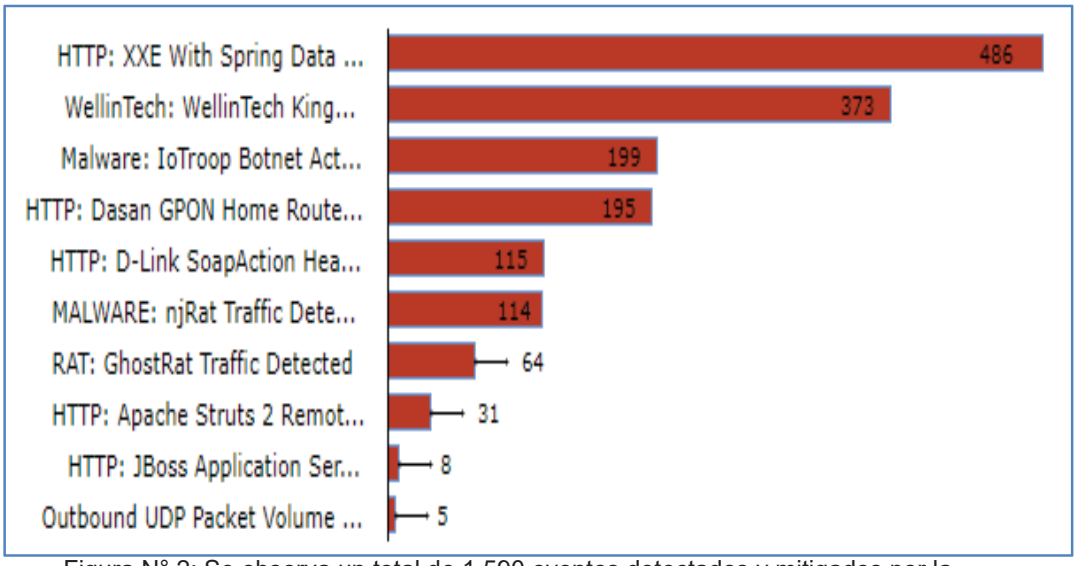


Figura N° 2: Se observa un total de 1,590 eventos detectados y mitigados por la herramienta IPS durante el mes de Octubre.

- Monitoreo Antimalware y antispam Office 365:

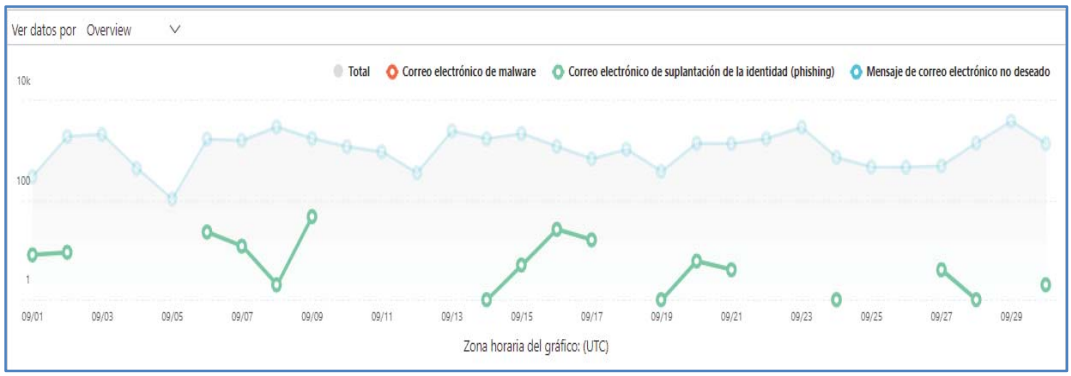


Figura N° 3: Se observa un total de 41,566 eventos detectados y mitigados por la herramienta antispam y antimalware de Office 365 en el mes de septiembre del presente año.

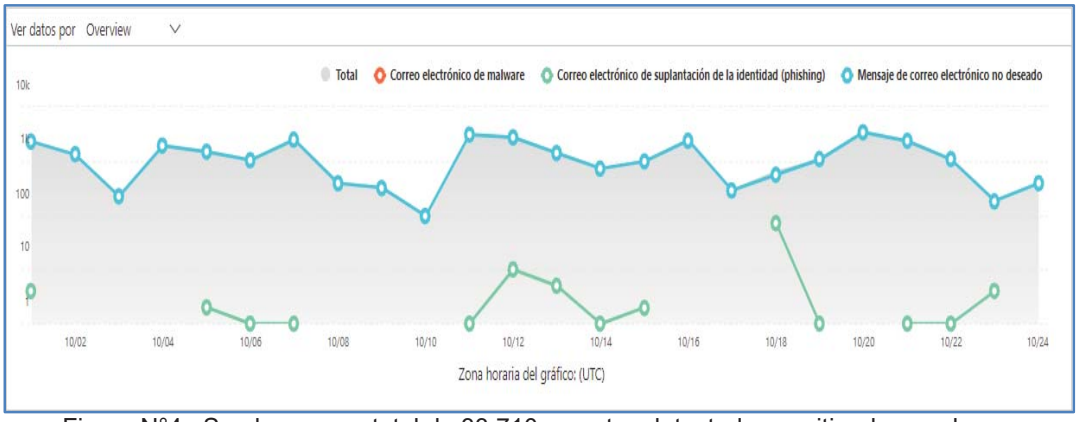
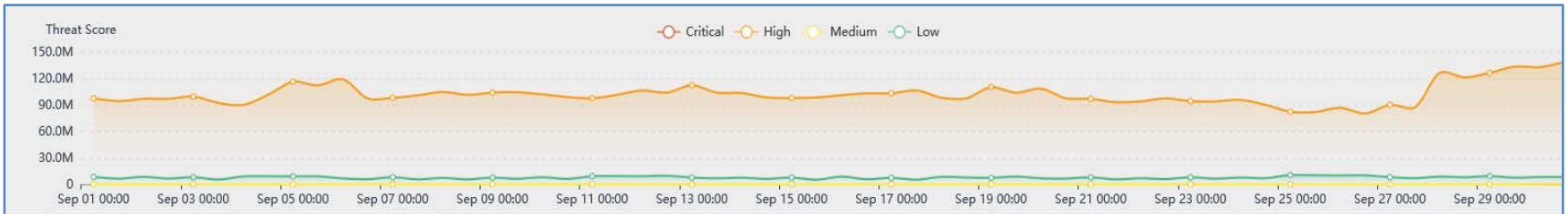


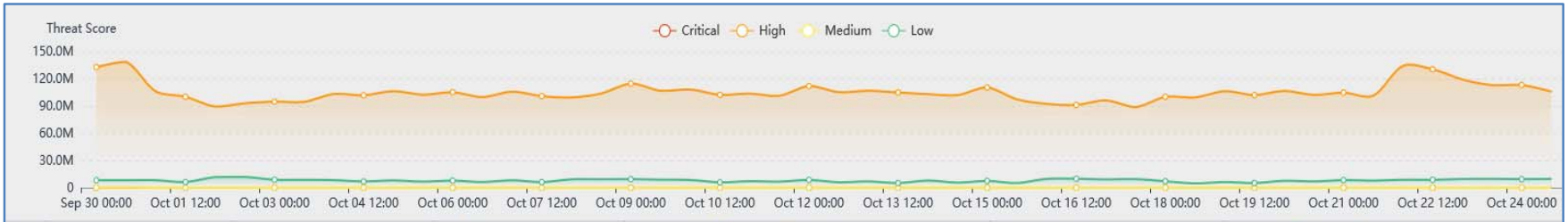
Figura N°4 : Se observa un total de 33,710 eventos detectados y mitigados por la herramienta antispam y antimalware de Office 365 en el mes de Octubre del presente año.

- Herramienta Firewall Perimetral:



#	Threat	Category	CVE ID	Threat Score(Blocked/ Allowed)	▼Threat Level	Incidents(Blocked/ Allowed)
1	Linksys.DirecTV.WVB.HTTP.He	IPS	CVE-2017-17411	100,950	Critical	2,019
2	udp_flood	IPS		13,150	Critical	263
3	Bash.Function.Definitions.Rem	IPS	CVE-2014-6271 CVE-2014-6	4,650	Critical	93
4	W32/Injector.EQDZ!tr	Malware		1,600	Critical	32
5	Apache.Struts.2.DefaultAction	IPS	CVE-2013-2251	550	Critical	11
6	Apache.Struts.2.OGNL.Script.I	IPS	CVE-2012-0391 CVE-2012-0	550	Critical	11
7	Apache.Struts.2.REST.Plugin.R	IPS	CVE-2016-4438 CVE-2017-1	550	Critical	11
8	Barco.OEM.Presentation.Platfc	IPS	CVE-2019-3929	550	Critical	11
9	Apache.Struts.2.Jakarta.Multip	IPS	CVE-2017-5638	550	Critical	11
10	OpenSSL.Heartbleed.Attack	IPS	CVE-2014-0160	350	Critical	7
11	tcp_port_scan	IPS		250	Critical	5
12	Java/GenericGB.29230!tr	Malware		200	Critical	4
13	Java.Debug.Wire.Protocol.Inse	IPS	CVE-2017-6639	200	Critical	4
14	HTML/Phish.1E95!tr	Malware		200	Critical	4
15	tcp_syn_flood	IPS		100	Critical	2
16	tcp_src_session	IPS		50	Critical	1
17	Netkit.Telnetd.IAC.Buffer.Over	IPS	CVE-2020-10188	50	Critical	1

Figura N°5 : Se observa un total de 2,490 eventos detectados y mitigados por la herramienta Firewall durante el mes de septiembre



#	Threat	Category	CVE ID	Threat Score(Blocked/ Allowed)	▼Threat Level	Incidents(Blocked/ Allowed)
1	Linksys.DirecTV.WVB.HTTP.He	IPS	CVE-2017-17411	99,950	Critical	1,999
2	udp_flood	IPS		16,500	Critical	330
3	Bash.Function.Definitions.Rem	IPS	CVE-2014-6271 CVE-2014-6	3,800	Critical	76
4	ip_src_session	IPS		1,200	Critical	24
5	W32/Injector.EQDZ!tr	Malware		300	Critical	6
6	OpenSSL.Heartbleed.Attack	IPS	CVE-2014-0160	300	Critical	6
7	tcp_port_scan	IPS		250	Critical	5
8	W32/Injector.EQGK!tr	Malware		200	Critical	4
9	Apache.Struts.2.DefaultAction	IPS	CVE-2013-2251	100	Critical	2
10	tcp_syn_flood	IPS		100	Critical	2
11	MSOffice/Scam.2ED7!tr	Malware		100	Critical	2
12	Apache.Struts.2.Jakarta.Multip	IPS	CVE-2017-5638	100	Critical	2
13	Apache.Struts.2.OGNL.Script.I	IPS	CVE-2012-0391 CVE-2012-0	100	Critical	2
14	Apache.Struts.2.REST.Plugin.R	IPS	CVE-2016-4438 CVE-2017-1	100	Critical	2
15	Barco.OEM.Presentation.Platfc	IPS	CVE-2019-3929	100	Critical	2
16	tcp_src_session	IPS		50	Critical	1
17	Blocked Connection Attempts	Blocked by Firewall Policy		5,255,624,970	High	175,187,499

Figura N°6: Se observa un total de 175,189,964 eventos detectados y mitigados por la herramienta Firewall durante el mes de Octubre.

- WAF On premise

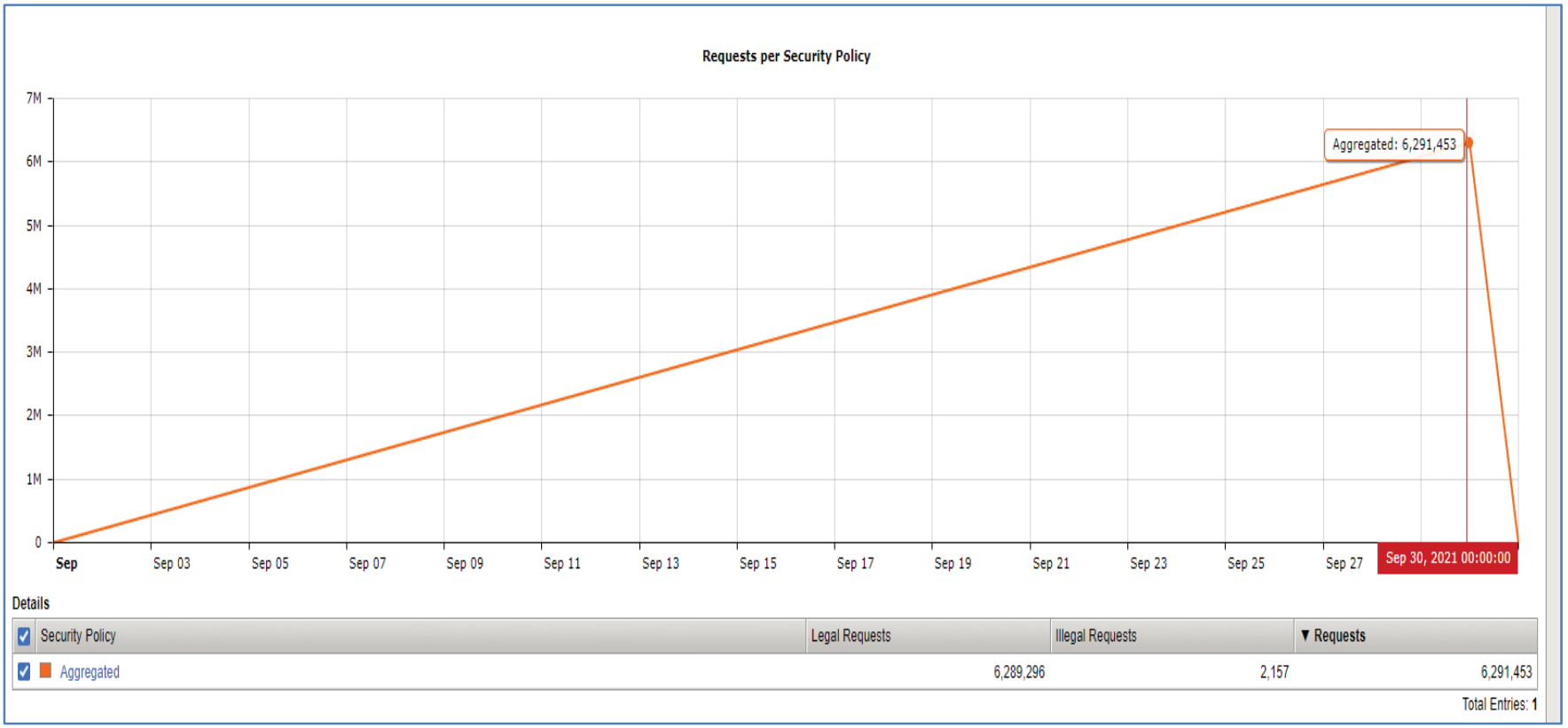


Figura N° 7: Se observa un total de 6,291,453 eventos detectados y mitigados por la herramienta WAF para aplicaciones On Premise durante el mes de septiembre.

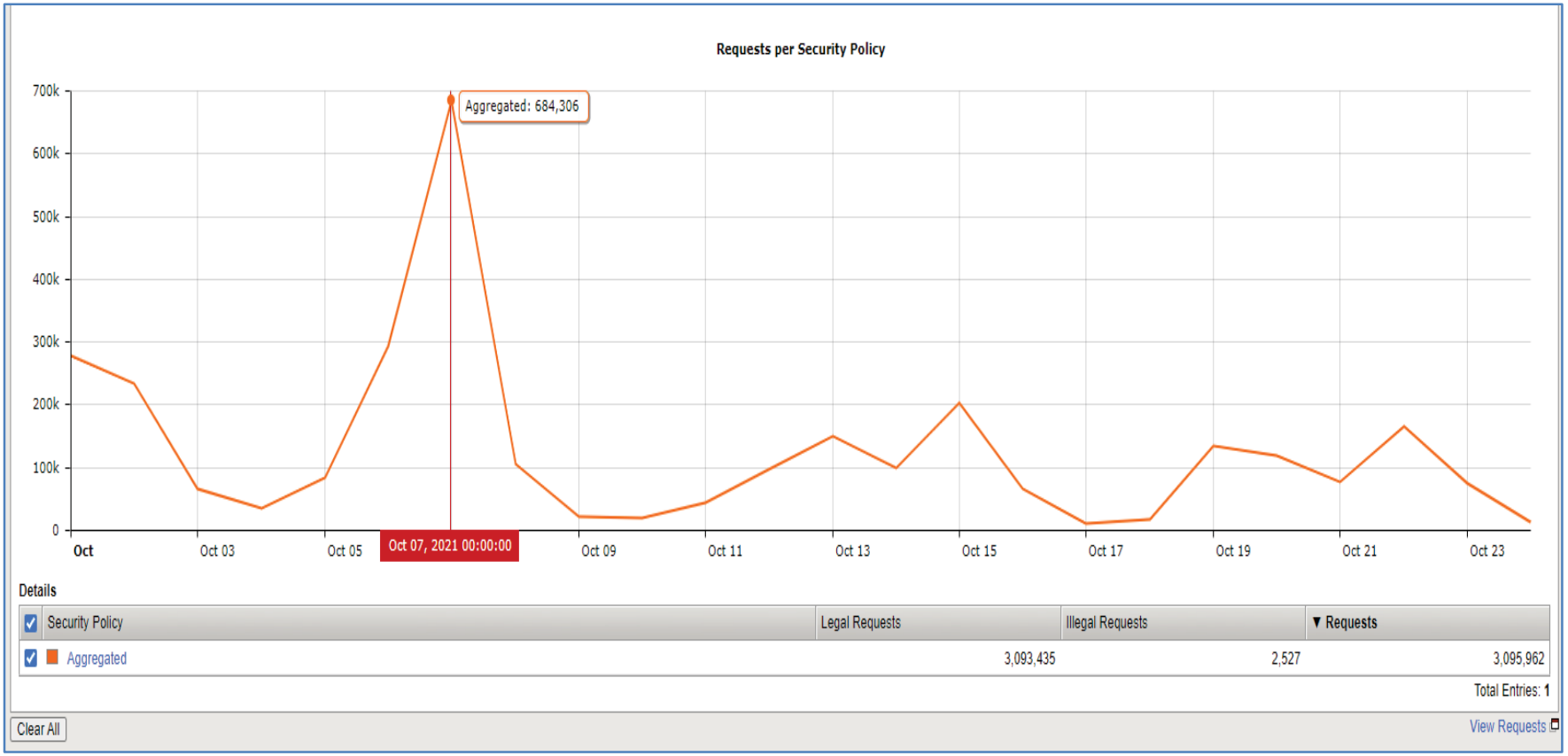


Figura N° 08: Se observa un total de 3,095,962 eventos detectados y mitigados por la herramienta WAF para aplicaciones On Premise durante el mes de octubre.

- Antimalware (Antivirus)

Acción	Virus	Spyware
Limpiado/bloqueado	0	1
Eliminado	89	2
En cuarentena	2	0
Sospechoso	0	0
Recientemente infectado	0	0
Aún infectado	0	0

Tabla 2: Se observa un total de 94 eventos detectados y mitigados por la herramienta antivirus durante el mes de Septiembre.

Acción	Virus	Spyware
Limpiado/bloqueado	6	0
Eliminado	2	12
En cuarentena	0	2
Sospechoso	0	0
Recientemente infectado	0	0
Aún infectado	0	0

Tabla 3: Se observa un total de 22 eventos detectados y mitigados por la herramienta antivirus durante el mes de Octubre.

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 dieron soporte a las EMC 2021.

Acción 2: Coordinar reuniones semanales con los integrantes del CSIRT Electoral.

Con fecha **23SEP2021** se realizó la primera reunión del CSIRT[1] electoral. Dicha reunión fue convocada por el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital en el marco de las Elecciones Municipales Complementarias realizadas el 10OCT2021.
La agenda desarrollada fue la siguiente:

1. Informe del CSIRT Perú
2. Coordinaciones de actividades del CSIRT electoral.

Importante anotar que en esta reunión se realizó la instalación del CSIRT electoral para el proceso electoral EMC 2021.

[1] El CSIRT electoral se conforma por iniciativa de los entes electorales (JNE, RENIEC y ONPE) y con el respaldo de la Secretaria de Gobierno Digital (SEGDI) de la Presidencia del Consejo de Ministros (PCM).

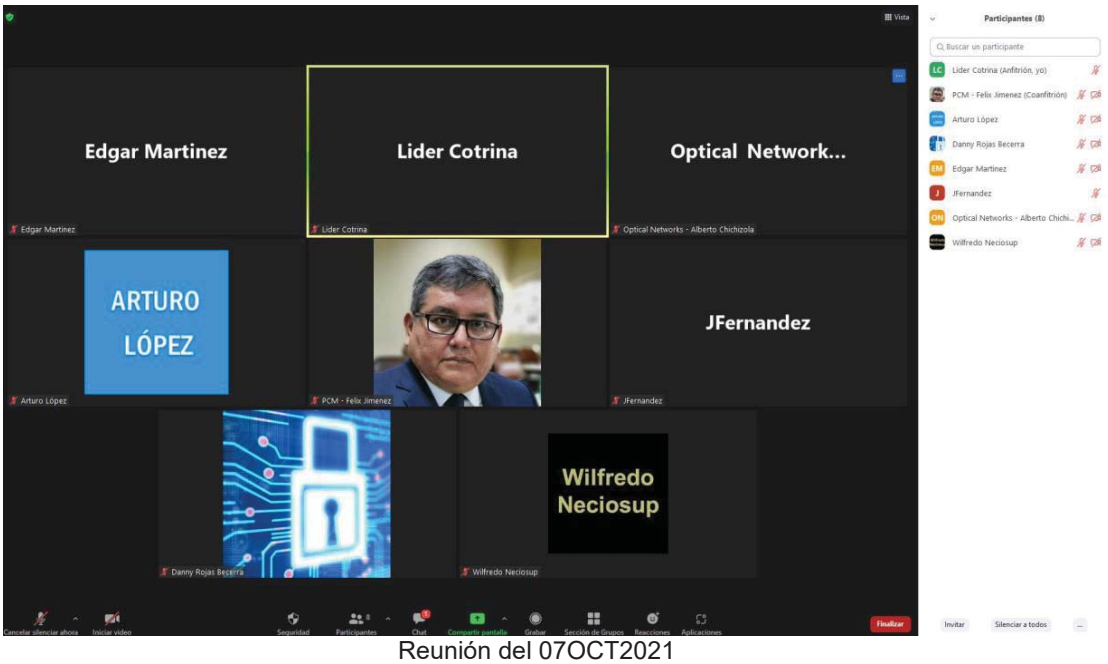
Reunión del 23SEP2021

Con fecha **29SEP2021**, el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital convoca para el **30SEP2021** la segunda reunión del CSIRT electoral.

- Agenda: Coordinación de las actividades del CISRT electoral.

Con fecha **06OCT2021**, la ONPE convoca para el **07OCT2021** la tercera reunión del CSIRT electoral:

- Agenda: Exposición de buenas prácticas en Ciberseguridad



Reunión del 07OCT2021

Acción 3: Realizar el seguimiento al monitoreo efectuado por los integrantes del CSIRT Electoral.

El monitoreo efectuado por los integrantes del CSIRT se realizó con herramientas que cada entidad posee y que forman parte de su infraestructura tecnológica.

Esta actividad permitió tener una cobertura de observación permanente para reportar cualquier incidente que hubiera ocurrido en los portales web publicados a internet por parte de los organismos electorales.

En ese sentido, realizado el monitoreo, los integrantes del CSIRT electoral **NO** reportaron la ocurrencia de incidentes de seguridad de la información relacionados a ciberataques.

	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 EMC 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		
									Sep 2021		Oct 2021					DESCRIPCIÓN DEL AVANCE / CUMPLIMIENTO	DIFICULTADES PRESENTADAS	MEDIDAS CORRECTIVAS
					Inicio	Fin	Inicio	Fin	Pr	Ej	Pr	Ej	META PROGRAMADA	META EJECUTADA	% AVANC			
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**	09/09/21	31/10/21			1	1	1	1	2	2	100%	**SETIEMBRE 2021:** Se realizó el monitoreo de las herramientas de Ciberseguridad detectándose **6,356,652** eventos **OCTUBRE 2021:** Se realizó el monitoreo de las herramientas de Ciberseguridad detectándose **178,321,248** eventos.	ninguna	ninguna
2	Coordinar reuniones semanales con los integrantes del CSIRT Electoral.	**SGIST**	**Reporte**	**Reporte**	23/09/21	31/10/21				1	1	1	1	2	200%	**SETIEMBRE 2021** **Se realizaron las siguientes reuniones:** • Con fecha **23SEP2021** se realizó la primera reunión del CSIRT[2] electoral. Dicha reunión fue convocada por el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital en el marco de las Elecciones Municipales Complementarias realizadas el 10OCT2021. **Agenda:** - Informe del CSIRT Perú - Coordinaciones de actividades del CSIRT electoral. • Con fecha **29SEP2021**, el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital convoca para el **30SEP2021** la segunda reunión del CSIRT electoral. **Agenda:** - Coordinación de las actividades del CISRT electoral. **OCTUBRE 2021:** **Se realizaron las siguientes reuniones:** • Con fecha **06OCT2021**, la ONPE convoca para el **07OCT2021** la tercera reunión del CSIRT electoral: **Agenda:** - Exposición de buenas prácticas en Ciberseguridad, ataques y peligros potenciales.	ninguna	ninguna
3	Realizar el seguimiento al monitoreo efectuado por los integrantes del CSIRT Electoral.	**SGIST**	**Reporte**	**Reporte**	23/09/21	31/10/21					1	1	1	1	100%	**OCTUBRE 2021**: Los integrantes del CSIRT ELECTORAL **NO** reportaron incidentes de ciberseguridad.	ninguna	ninguna

[2] El CSIRT electoral se conforma por iniciativa de los entes electorales (JNE, RENIEC y ONPE) y con el respaldo de la Secretaria de Gobierno Digital (SEGDI) de la Presidencia del Consejo de Ministros (PCM).

III. BALANCE GENERAL

3.1. Logros Obtenidos

Con respecto al objetivo de lo programado:

- Evitar incidentes a los activos informáticos que dan soporte a las EMC 2021.

Se aprecia el siguiente resultado en el indicador:

Indicador 1: Porcentaje de eventos de Ciberseguridad bloqueados.

$$\left[\frac{X*100\,\%}{X+Y}\right] = \left[\frac{184'677{,}900*100\%}{184'677{,}900+0}\right]$$

Meta: 98% **Resultado:** 100%

X= Número de eventos de Ciberseguridad bloqueados = 184'677,900.
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.

Con respecto a las actividades operativas y/o acciones del PLAN:

Las acciones programadas y ejecutadas se aprecian en la siguiente tabla:

Tareas	Cantidad
Programadas	3
Ejecutadas	3

Tabla N° 5: Tareas

Logros:

Se realizó el monitoreo permanente de las aplicaciones electorales publicadas en internet.

Se mitigaron todos los intentos de ataques a la infraestructura electoral expuesta a internet.

3.2. Problemas identificados y medidas correctivas adoptadas

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

IV. EJECUCIÓN DEL PRESUPUESTO

El presupuesto en el incurre para la ejecución del "PLAN DE CIBERSEGURIDAD EMC 2021" comprende el trabajo del capital humano establecido en la partida del gasto 2.3.28.1 Contrato Administrativo de Servicios, correspondiente al personal CAS", el cual está comprendido al Presupuesto Institucional que tiene la meta 0028 GITE.

Actividad	Ejecutor	Sueldo Mensual (S/.)	Sueldo /Hora	Número de Horas	Sub Total (S/.)
Monitorear las herramientas de Ciberseguridad	Especialista en Telecomunicaciones	6000	25	51	S/.1275.00
Coordinar reuniones semanales con los integrantes del CSIRT Electoral	Especialista en Telecomunicaciones	6000	25	16	S/.400.00
Realizar el seguimiento al monitoreo efectuado por los integrantes del CSIRT Electoral	Especialista en Telecomunicaciones	6000	25	24	S/.600.00
Total					**2,275**

Tabla N° 6: Presupuesto

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 las EMC 2021.
- Se mitigó un total de 184’677,900 eventos de seguridad tal como se muestran en la Tabla N° 1.

Recomendaciones:

Se recomienda continuar con el monitoreo permanente de los eventos de Ciberseguridad con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la información de la entidad.