INFORME DE EVALUACIÓN

PLAN DE CIBERSEGURIDAD PARA EL PROCESO ELECTORAL ELECCIONES REGIONALES Y MUNICIPALES 2022

Plan Especializado

Elaborado por:

Gerencia de Informática y Tecnología Electoral

LIMA, OCTUBRE 2023

INDICE

ABREVIATURAS

LISTADO DE NOMBRES	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
Elecciones Regionales y Municipales 2022	ERM 2022
Sistema de Prevención de Intrusos	IPS
Equipos de respuesta ante Incidentes de Seguridad Digital	ERISD

I. RESUMEN EJECUTIVO

La finalidad del presente informe es evaluar lo establecido en el "Plan de Ciberseguridad para el proceso electoral Elecciones Regionales y Municipales 2022 aprobado con Resolución Gerencial N.º 000002-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 Regionales y Municipales 2022.

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 ERM 2022. Además, es preciso indicar que, se logró superar la meta programada del 98%, obteniendo un 100% de eventos de Ciberseguridad bloqueados en el periodo Julio – Octubre del 2022, con un total de 7,739,175 eventos detectados y mitigados por las herramientas de Ciberseguridad.

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

Como parte de la evaluación de las acciones y/o actividades operativas se detalla el resultado del indicador, cuyos eventos se encuentran descritos en la tabla N°3:

Indicador: Porcentaje de eventos de Ciberseguridad bloqueados.

$$\left[\frac{X*100\%}{X+Y}\right]$$

Meta = 98%

X = Número de eventos de Ciberseguridad bloqueados
Y = Número de Incidentes que afectaron los activos de información y servicios informáticos

Porcentaje de eventos de Ciberseguridad bloqueados	$\frac{7,739,175 * 100\%}{7,739,175 + 0} = 100\%$

En el numeral VIII. Acciones del PLAN, se establece lo siguiente:

15. Cód.	16. Actividad Operativa / Tarea / Acción
1	Gestionar servicios relacionados a Ciberseguridad y monitorear las herramientas de Ciberseguridad
2	Coordinar reuniones semanales con los integrantes del CSIRT Electoral.

Tabla N° 1: Lista de actividades del PLAN

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

	FORMATO	Código:	FM11-GPP/PLAN
		Versión:	04
	EVALUACIÓN DE PLANES ESPECIALIZADOS Y DE ACCIÓN	Fecha de aprobación:	15/02/2018
		Página:	1 de 1

1. NOMBRE DEL PLAN -AÑO:	**Plan de Ciberseguridad ERM2022**
2. ORGANO RESPONSABLE:	**Gerencia de Informática y Tecnología Electoral**

15 Código	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		
									Jul 2022		Ago 2022		Set 2022		Oct 2022							
					Inicio	Fin	Inicio	Fin	Pr	Ej	Pr	Ej	Pr	Ej	Pr	Ej	META PROGRAMADA	META EJECUTADA	% AVANCE	DESCRIPCIÓN DEL AVANCE / CUMPLIMIENTO	DIFICULTADES PRESENTADAS	MEDIDAS CORRECTIVAS
II	**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	Gestionar servicios relacionados a Ciberseguridad y monitorear las herramientas de Ciberseguridad	SGIST	Reporte	Reporte	01/09/22	31/10/22	01/07/22	31/10/22		1		1	1	1	1	1	2	4	100%	Se gestionaron los servicios de ciberseguridad como Servicio de Ethical Hacking ERM 2022, IPS, Antispam Ofifice 365, Firewall Perimetral, Anti-Denegación de Servicios, Firewall de Aplicaciones Web Cloud, Firewall de Aplicaciones Web On Premise, Antimalware. De forma diaria se realizó el monitoreo de las herramientas de ciberseguridad para detectar amenazas desde julio a octubre 2022.	ninguna	ninguna
2	Coordinar reuniones semanales con los integrantes del CSIRT Electoral.	SGIST	Reporte	Reporte	01/09/22	31/10/22	30/09/22	28/10/22					1	1	1	1	2	2	100%	Se realizaron las reuniones con el equipo de respuesta a incidentes de seguridad digital ERISD-ONPE Temas tratados: • Estrategia de Ciberseguridad ERM 2022 • Inventario de Activos de información. • Capacitación y Concientización • Fases de Ciclo de Respuesta a Incidentes de Seguridad según NIST.	ninguna	ninguna

Tabla N° 2: Evaluación de las actividades del PLAN

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

Actividad 1: Gestionar servicios relacionados a Ciberseguridad y monitorear las herramientas de Ciberseguridad

2.1. Monitoreo de herramientas de Ciberseguridad

Acciones Realizadas

Durante los meses de Julio, Agosto, Setiembre y Octubre del 2022 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 de información que dieron soporte a las Elecciones Regionales y Municipales 2022. A continuación, semuestra en una tabla resumen que consolida los eventos registrados desde el inicio del servicio de monitoreo de las aplicaciones electorales publicadas a Internet:

Herramienta	Julio	Agosto	Setiembre	Octubre	Suma de eventos
Sistema de prevención de Intrusos (IPS)	**545,818**		**569,402**		**1,115,220**
Antispam Office 365	*	*	**35,692**	**24,145**	**59,837**
Firewall Perimetral	**1,769**	**1,794**	**1,833**	**1,886**	**7,282**
Anti-Denegación de Servicios	0	0	0	0	**0**
Firewall de Aplicaciones Web Cloud	*	*	**164,854**	**108,324**	**273,178**
Firewall de Aplicaciones Web On premise	**6,283,393**				**6,283,393**
Antimalware (Antivirus)	**39**	**11**	**215**		**265**
	Total de Eventos				**7,739,175**

Tabla N° 3: Total de 7,739,175 eventos detectados y mitigados por las herramientas de Ciberseguridad.

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

A. Monitoreo del Sistema de prevención de Intrusos (IPS):

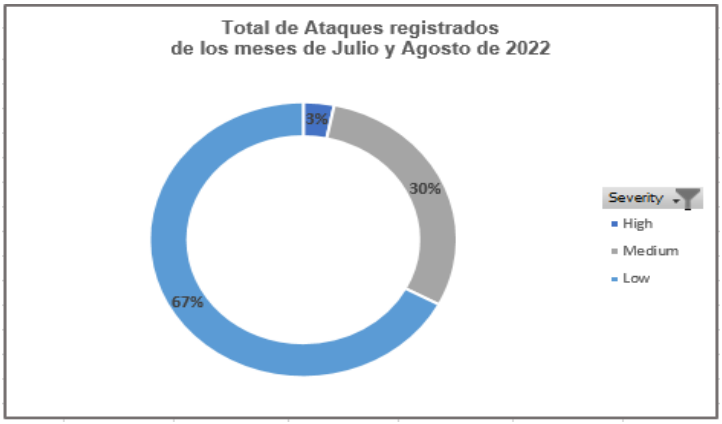


Figura N° 1: Se observa un total de 545, 818 eventos detectados y mitigados por laherramienta IPS durante Julio y Agosto 2022.

Severidad	Cantidad	Porcentaje
High	17, 682	3%
Medium	161, 409	30%
Low	366, 727	67%
Total	**545, 818**	**100%**

Tabla N° 4: Resumen cantidad de eventos por severidad de la herramienta IPS durante Julio y Agosto 2022

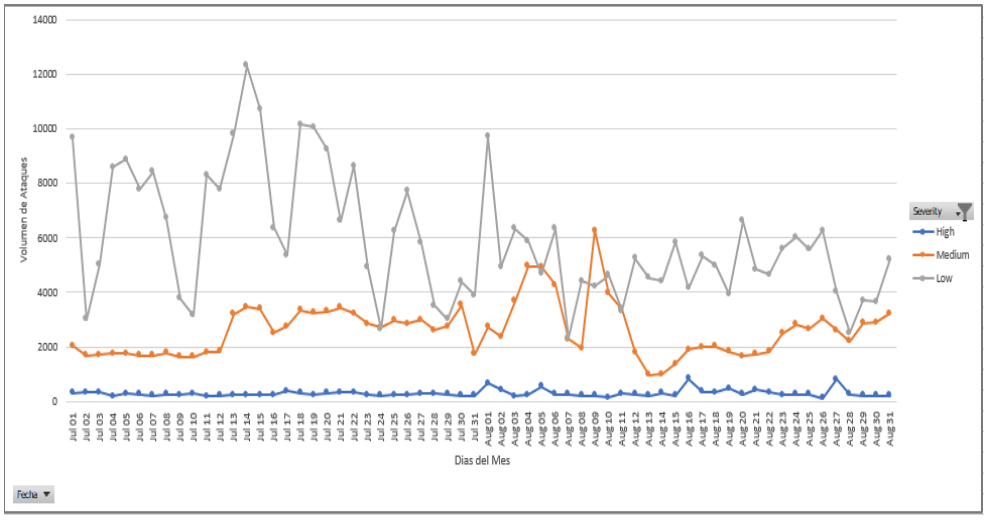


Figura N° 2.- Línea de tiempo de los ataques de Julio y Agosto 2022 donde se resalta ataques en LOW los días 14 y 18 de julio 2022

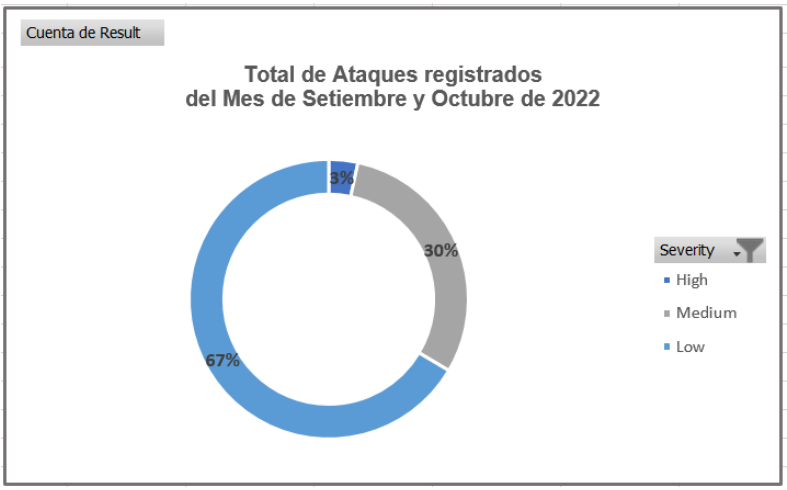


Figura N° 3: Se observa un total de 569, 402 eventos detectados y mitigados por laherramienta IPS durante Setiembre y Octubre 2022.

Severidad	Cantidad	Porcentaje
High	19, 167	3%
Medium	171, 730	30%
Low	378, 505	67%
Total	**569, 402**	**100%**

Tabla N° 5: Resumen cantidad de eventos por severidad de la herramienta IPS durante Setiembre y Octubre 2022

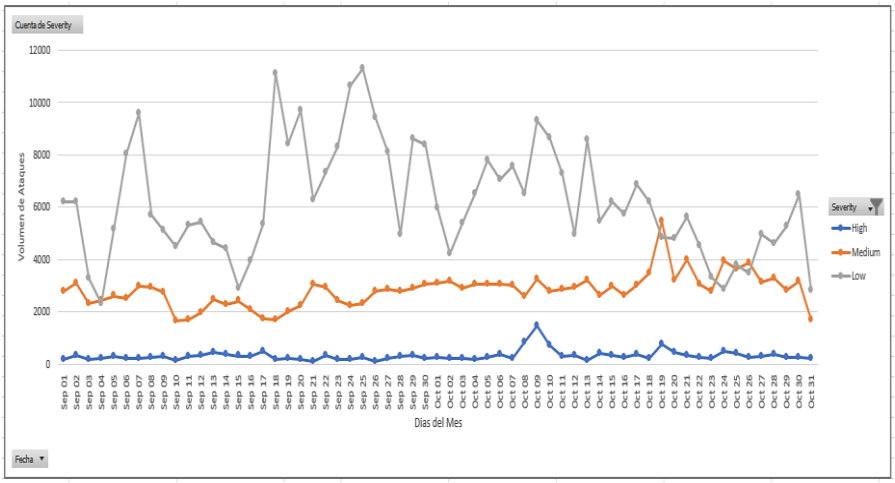


Figura N.° 4.- Línea de tiempo de los ataques de Setiembre y Octubre 2022 donde se resalta actividad crítica pronunciada los días 18 y 25 de setiembre en calidad de low (bajo).

B. Monitoreo Antimalware y Antispam Office 365:

Figura N° 5: Se observa un total de 35, 692 eventos detectados y mitigados por la herramienta antispam y antimalware de Office 365 en Setiembre 2022

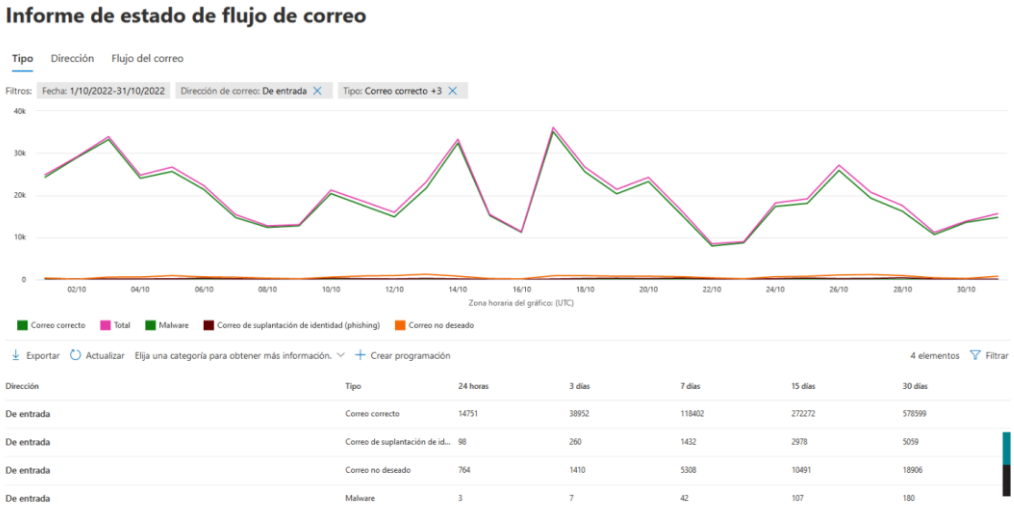


Figura N.º 6: Se observa un total de 24,145 eventos detectados y mitigados por la herramienta antispam y antimalware de Office 365 en Octubre

C. Herramienta Firewall Perimetral:

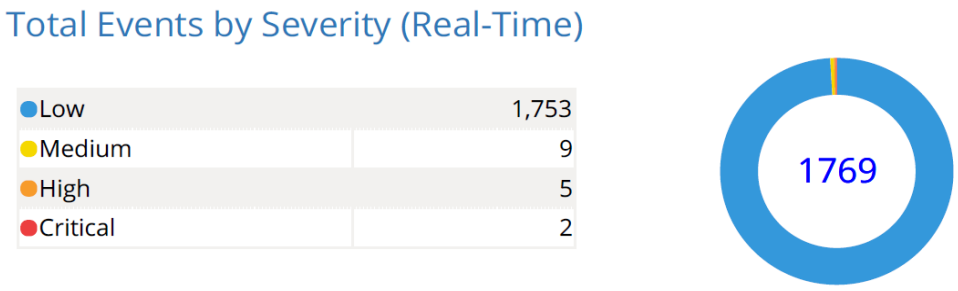


Figura N° 7: Se observa un total de 1,769 eventos detectados y mitigados por la herramienta firewall perimetral durante el mes de julio.

#	Severity	Event Name	Events Occurrences	% of Subtotal
1	Low	Default-Risky-Destination-Detection-By-Threat	1,736	99.03%
		Default-Risky-Destination-Detection-By-Endpoint	16	0.91%
		Default-Risky-App-Detection-By-Endpoint	1	0.06%
		Subtotal	**1,753**	**99.10%**
2	Medium	Default-Malicious-Code-Detection-By-Threat	3	33.33%
		Default-Risky-Destination-Detection-By-Threat	3	33.33%
		Default-Risky-Destination-Detection-By-Endpoint	2	22.22%
		Others	**1**	**11.11%**
		Subtotal	**9**	**0.51%**
3	High	Default-Malicious-Code-Detection-By-Endpoint	3	60.00%
		Default-Risky-Destination-Detection-By-Endpoint	1	20.00%
		Default-Risky-Destination-Detection-By-Threat	1	20.00%
		Subtotal	**5**	**0.28%**
4	Critical	Default-Compromised Host-Detection-IOC-By-Endpoint	1	50.00%
		Default-Compromised Host-Detection-IOC-By-Threat	1	50.00%
		Subtotal	**2**	**0.11%**
	Total		**1,769**	**100.00%**

Tabla N° 6: Total 1,769 de eventos ocurridos por severidad y categoría para el mes de julio.

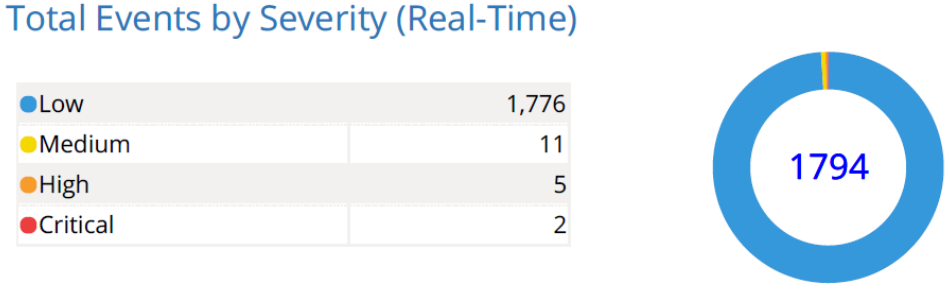


Figura N° 7: Se observa un total de 1,794 eventos detectados y mitigados por la herramienta firewall perimetral durante el mes de agosto.

#	Severity	Event Name	Events Occurrences	% of Subtotal
1	Low	Default-Risky-Destination-Detection-By-Threat	1,759	99.04%
		Default-Risky-Destination-Detection-By-Endpoint	16	0.90%
		Default-Risky-App-Detection-By-Endpoint	1	0.06%
		Subtotal	**1,776**	**99.00%**
2	Medium	Default-Risky-Destination-Detection-By-Threat	4	36.36%
		Default-Malicious-Code-Detection-By-Threat	3	27.27%
		Default-Risky-Destination-Detection-By-Endpoint	3	27.27%
		Others	**1**	**9.09%**
		Subtotal	**11**	**0.61%**
3	High	Default-Malicious-Code-Detection-By-Endpoint	3	60.00%
		Default-Risky-Destination-Detection-By-Endpoint	1	20.00%
		Default-Risky-Destination-Detection-By-Threat	1	20.00%
		Subtotal	**5**	**0.28%**
4	Critical	Default-Compromised Host-Detection-IOC-By-Endpoint	1	50.00%
		Default-Compromised Host-Detection-IOC-By-Threat	1	50.00%
		Subtotal	**2**	**0.11%**
	Total		**1,794**	**100.00%**

Tabla Nº 7: Total 1,794 de eventos ocurridos por severidad y categoría para el mes de agosto.

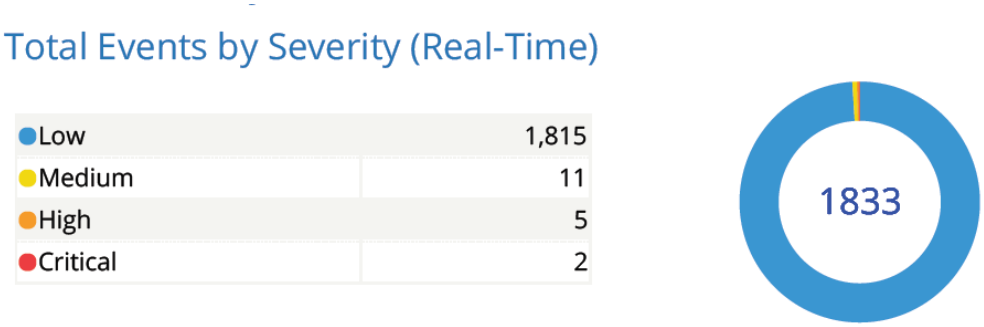


Figura N° 7: Se observa un total de 1,833 eventos detectados y mitigados por la herramienta firewall perimetral durante el mes de setiembre.

#	Severity	Event Name	Events Occurrences	% of Subtotal
1	Low	Default-Risky-Destination-Detection-By-Threat	1,798	99.06%
		Default-Risky-Destination-Detection-By-Endpoint	16	0.88%
		Default-Risky-App-Detection-By-Endpoint	1	0.06%
		Subtotal	**1,815**	**99.02%**
2	Medium	Default-Risky-Destination-Detection-By-Threat	4	36.36%
		Default-Malicious-Code-Detection-By-Threat	3	27.27%
		Default-Risky-Destination-Detection-By-Endpoint	3	27.27%
		Others	**1**	**9.09%**
		Subtotal	**11**	**0.60%**
3	High	Default-Malicious-Code-Detection-By-Endpoint	3	60.00%
		Default-Risky-Destination-Detection-By-Endpoint	1	20.00%
		Default-Risky-Destination-Detection-By-Threat	1	20.00%
		Subtotal	**5**	**0.27%**
4	Critical	Default-Compromised Host-Detection-IOC-By-Endpoint	1	50.00%
		Default-Compromised Host-Detection-IOC-By-Threat	1	50.00%
		Subtotal	**2**	**0.11%**
	Total		**1,833**	**100.00%**

Tabla Nº 8: Total 1,833 de eventos ocurridos por severidad y categoría para el mes de setiembre.

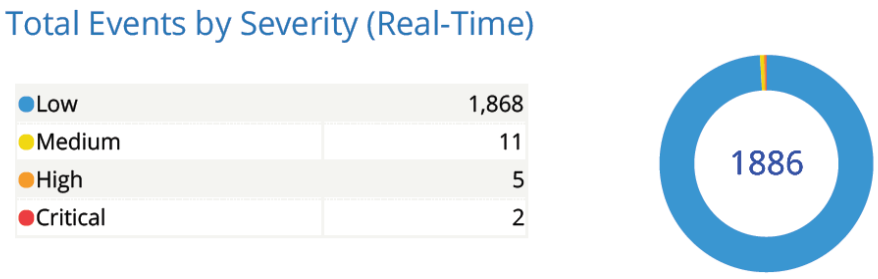


Figura N° 7: Se observa un total de 1,886 eventos detectados y mitigados por la herramienta firewall perimetral durante el mes de octubre.

#	Severity	Event Name	Events Occurrences	% of Subtotal
1	Low	Default-Risky-Destination-Detection-By-Threat	1,850	99.04%
		Default-Risky-Destination-Detection-By-Endpoint	17	0.91%
		Default-Risky-App-Detection-By-Endpoint	1	0.05%
		Subtotal	**1,868**	**99.05%**
2	Medium	Default-Risky-Destination-Detection-By-Threat	4	36.36%
		Default-Malicious-Code-Detection-By-Threat	3	27.27%
		Default-Risky-Destination-Detection-By-Endpoint	3	27.27%
		Others	**1**	**9.09%**
		Subtotal	**11**	**0.58%**
3	High	Default-Malicious-Code-Detection-By-Endpoint	3	60.00%
		Default-Risky-Destination-Detection-By-Endpoint	1	20.00%
		Default-Risky-Destination-Detection-By-Threat	1	20.00%
		Subtotal	**5**	**0.27%**
4	Critical	Default-Compromised Host-Detection-IOC-By-Endpoint	1	50.00%
		Default-Compromised Host-Detection-IOC-By-Threat	1	50.00%
		Subtotal	**2**	**0.11%**
	Total		**1,886**	**100.00%**

Tabla Nº 9: Total 1,886 de eventos ocurridos por severidad y categoría para el mes de octubre.

D. Anti-Denegación de Servicios

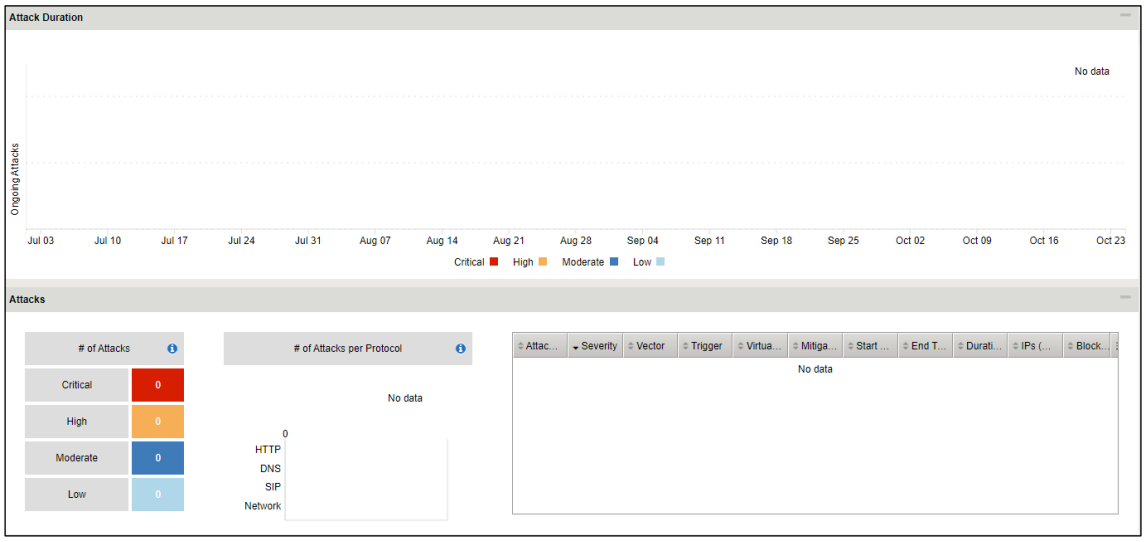


Figura N° 8: Se observa que no hubo eventos detectados en la herramienta Anti-Denegación de servicios durante los meses de Julio a Octubre 2022

E. Firewall de Aplicaciones Web Cloud

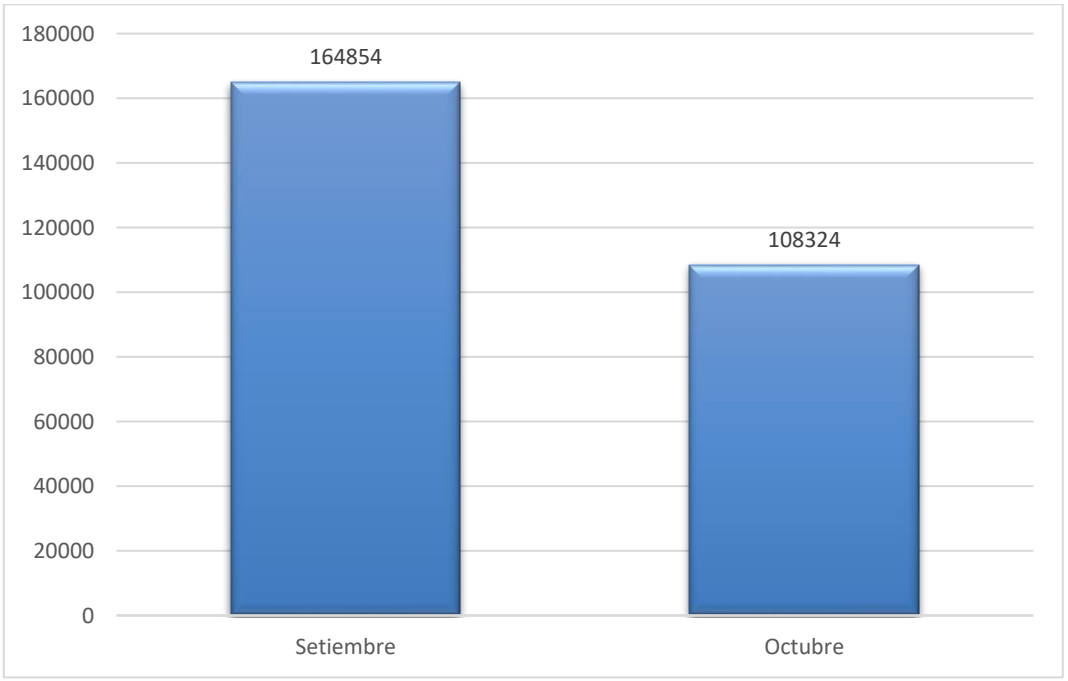


Figura N° 9.- Se observa un total de 273,178 de eventos detectados y mitigados por la herramienta WAF para aplicaciones durante los meses de Setiembre y Octubre 2022.

F. Firewall de Aplicaciones Web On premise

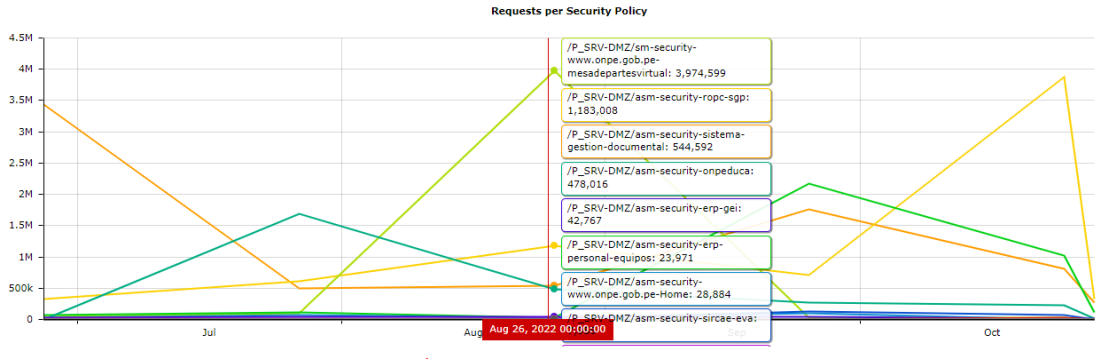


Figura N° 14: Se observa un total de 6,283,393 eventos detectados y mitigados por la herramienta WAF para aplicaciones On-Premise durante Julio, Agosto, Setiembre y Octubre 2022.

G. Antimalware (Antivirus)

Acción	Virus	Spyware
Limpiado	2	22
Eliminado	0	0
En cuarentena	15	0
Omitido	0	0
Nombre modificado	0	0
Acción necesaria	0	0
TOTAL	17	22

Tabla N° 10: Se observa un total de 39 eventos detectados y mitigados por la herramienta antivirus Trend Micro durante el mes de Julio 2022.

Acción	Virus	Spyware
Limpiado	5	2
Eliminado	0	0
En cuarentena	2	1
Omitido	0	0
Nombre modificado	0	0
Acción necesaria	1	0
TOTAL	8	3

Tabla N° 11: Se observa un total de 11 eventos detectados y mitigados por la herramienta antivirus Trend Micro durante el mes de Agosto 2022

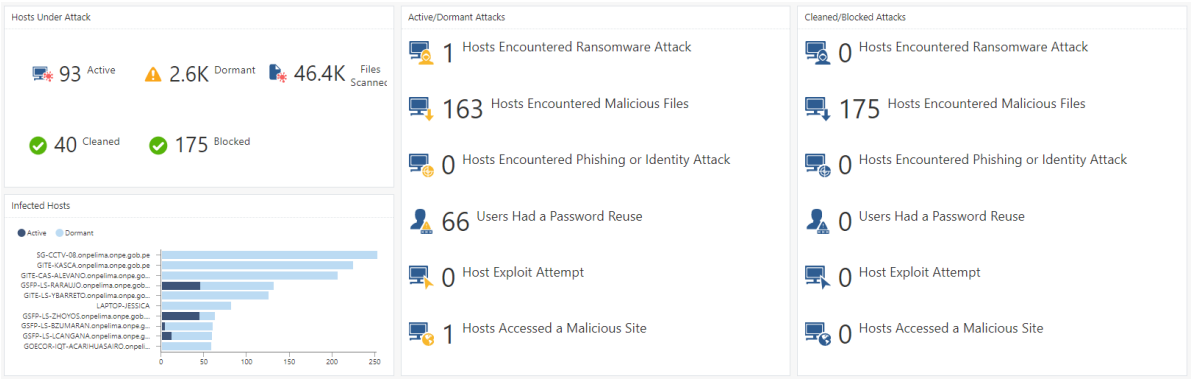


Figura N° 9: Se observa un total de 215 eventos detectados y mitigados por la herramienta antivirus Harmony endpoint durante el mes de Setiembre y Octubre 2022.

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 Elecciones Regionales y Municipales - ERM 2022.

Así mismo, **algunos eventos detectados entre el 29JUN2022 y 05NOV2022 fueron debido a la ejecución del "Servicio Ethical Hacking ERM 2022".** Tal como indica en el siguiente cronograma entregado por el proveedor servicios

ETAPA	Inicio	Fin
INICIO DEL SERVICIO	29/06/2022	29/06/2022
PLAN DE TRABAJO – ENTREGABLE 1	03/07/2022	03/07/2022
EJECUCION DE ESCENARIOS Y ANALISIS	30/06/2022	30/06/2022
INFORMES TECNICOS, EJECUTIVO Y MATRIZ DE VULNERABILIDADES	01/07/2022	05/07/2022
ENTREGA DE INFORMES – ENTREGABLE 2	05/07/2022	05/07/2022
EJECUCION DE ESCENARIOS Y ANALISIS	01/07/2022	31/08/2022
INFORMES TECNICOS, EJECUTIVO Y MATRIZ DE VULNERABILIDADES	01/09/2022	05/09/2022
ENTREGA DE INFORMES – ENTREGABLE 3	05/09/2022	05/09/2022
EJECUCION DE ESCENARIOS Y ANALISIS	01/09/2022	31/10/2022
INFORMES TECNICOS, EJECUTIVO Y MATRIZ DE VULNERABILIDADES	01/11/2022	05/11/2022
ENTREGA DE INFORMES – ENTREGABLE 4	05/11/2022	05/11/2022

Tabla N° 12: Cronograma de actividades del Servicio Ethical Hacking ERM 2022.

2.2. Gestionar servicios Relacionados a Ciberseguridad

Durante el presente año se realizó el Servicio de Ethical Hacking entre desde 29 de junio al 05 de noviembre de 2022, y se tienen los entregables en el Anexo (A) del documento. Se realizo el servicio tomando como alcance los siguientes puntos:

Tipo	Descripción	Cantidad
Infraestructura	b.1 Equipos de red y de seguridad perimetral (ej.: switch, router, IPS, firewall). b.2 Servidores de red (ej.: control de acceso a la red, antivirus, logs, monitoreo, mensajería de cola, NTP, sellado de tiempo). b.3 Servidores de aplicaciones (sistema operativo y plataforma de servidor de aplicaciones) b.4 Servidores de base de datos (sistema operativo y plataforma de base de datos). b.5 Estaciones de trabajo. b.6 Módulo de seguridad basado en hardware (HSM – TSA).	90
Aplicaciones	b.7 Aplicaciones web y de escritorio.	50
Equipos de local de votación - STAE	b.8 Laptop de escrutinio automatizado. b.9 Laptop de transmisión.	2

Tabla N°13: Activos del alcance del servicio de Ethical Hacking ERM 2022

N°	Origen de Ataque	Objetivo de Ataque
1	Desde la internet.	Activos de Aplicaciones web de la Red Administrativa - DMZ involucradas en el desarrollo del proceso electoral.
2	Desde la internet.	Activos de la Red Electoral.
3	Desde la Red Administrativa en la sede central	Activos de la Red Electoral.
4	Desde la Red Administrativa en la sede central	Activos de Aplicaciones web de la Red Administrativa involucradas en el desarrollo del proceso electoral.
5	Desde la Red Administrativa de la ODPE	Activos de la Red Electoral.
6	Desde la Red Electoral en el centro de cómputo	Activos de Infraestructura de la Red Electoral en la sede central
7	Desde la Red Electoral en el centro de cómputo	Activos de Infraestructura de la Red Electoral en el centro de cómputo
8	Desde la Red Electoral en la sede central	Activos de Infraestructura de la Red Electoral en el centro de cómputo.
9	Desde la Red Electoral en la sede central	Activos de Infraestructura de la Red Electoral en la sede central.
10	Desde la red de personalización de dispositivos de voto electrónico STAE	Activos de la red de preparación de equipos y dispositivos de voto electrónico STAE.

N°	Origen de Ataque	Objetivo de Ataque
11	Desde la oficina o ambiente en donde se ubican los activos (acceso físico)	Activos de equipos de local de votación – STAE
12	Desde la oficina o ambiente en donde se ubican los activos (acceso físico)	Activos de aplicaciones de escritorio.

Tabla N°14: Escenarios del alcance del servicio de Ethical Hacking ERM 2022

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

Acciones realizadas:

Conforme a la Resolución de Gerencia General N° 000073-2021-GG/ONPE, se constituye el "Equipo de Respuestas ante Incidentes de Seguridad Digital de la Oficina Nacional de Procesos Electorales", como responsables de gestionar los eventos o incidentes de seguridad digital. Por lo cual el equipo de respuesta a incidentes de seguridad digital fue conformado por los integrantes de las distintas Subgerencias de GITE. A continuación, se muestra las reuniones llevadas a cabo que dieron inicio el 30SEP2022 hasta 28OCT2022; las reuniones fueron llevadas a cabo por Microsoft Teams.

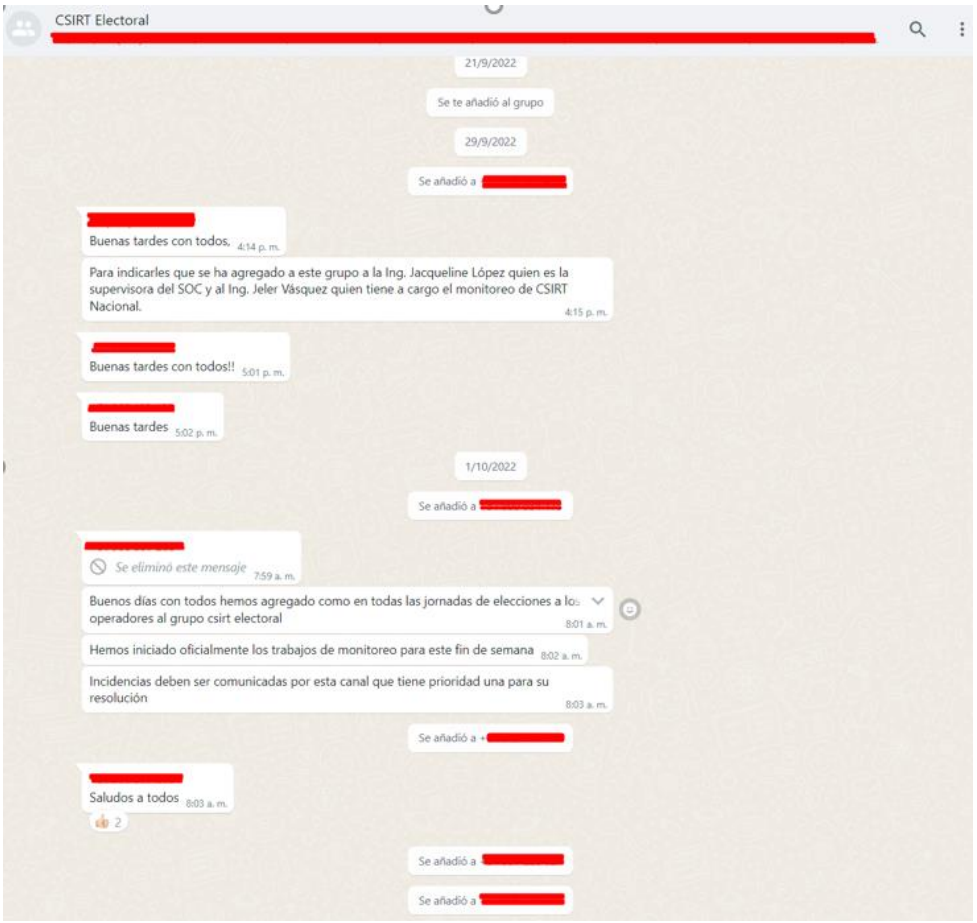
Figura 13.- Reunión ejecutada el día 30SET2022 con el equipo ERISD-ONPE.

Las agendas desarrolladas fueron las siguientes:

Fecha	Titulo	Agenda
30/09/2022	Equipos de Respuesta a Incidentes de Seguridad Digital ERISD-ONPE & Evaluación Plan de Ciberseguridad	- Revisión de informes pendientes del plan de ciberseguridad ERM 2022 - Estrategia de Ciberseguridad - Servicios Actuales de Ciberseguridad - Inventario de Activos de información
7/10/2022	Plan de Ciberseguridad ERM 2022 - Equipos de respuestas ante Incidentes de Seguridad Digital	- Revisión Plan de Ciberseguridad ERM 2022. - Objetivos - Conformación del Equipos Respuesta Incidentes ERISD-ONPE - Estrategia de Ciberseguridad según Marco NIST - Siguientes pasos
14/10/2022	Equipo de Respuesta a Incidentes de Seguridad Digital ERISD-ONPE	- Revisión de Evaluación de Plan Ciberseguridad ERM 2022 - Tecnologías actuales de Ciberseguridad de ONPE - Capacitación y Concientización - Inventario de Activos de Información
21/10/2022	Equipos de Respuesta ante Incidentes de Seguridad Digital ERISD-ONPE	- Revisión del Plan Ciberseguridad ERM 2022 - Revisión del Servicio de Ethical Hacking - Capacitación y Concientización - Inventario de Activos de Información
28/10/2022	Equipos de Respuesta ante Incidentes de Seguridad Digital ERISD-ONPE	- Revisión del Plan Ciberseguridad ERM 2022 - Revisión del Servicio de Ethical Hacking - Vulnerabilidades detectadas en EH - Ejercicios de simulación ante ciberataques. - Inventario de activos críticos de Información

Tabla N°15: Listado de agenda de reuniones realizadas.

Adicionalmente, se informó que se está habilitando el monitoreo CISRT Nacional para el fin de semana electoral, como se detalla en el grupo de WhatsApp.



III. BALANCE GENERAL

3.1. Logros Obtenidos

Con respecto al objetivo de lo programado:

- Se supero la meta del 98%, logrando el 100% de eventos de ciberseguridad bloqueados y/o mitigados para el Proceso Electoral ERM 2022.

3.2. Problemas identificados y medidas correctivas adoptadas

No se presentaron inconvenientes durante la ejecución del Plan de Ciberseguridad ERM 2022.

IV. EJECUCIÓN DEL PRESUPUESTO

El presupuesto en el incurre para la ejecución del “PLAN DE CIBERSEGURIDAD ERM 2022” comprende el trabajo del capital humano establecido en la partida del gasto 2.3.2.9.1.1 Contrato Administrativo de Servicios. Considerando el pago mensual del personal asignado como “Servicio de Locador de servicio de Especialista de Ciberseguridad”:

N° ITEM	Detalle del presupuesto requerido pera el Plan de Ciberseguridad ERM 2022	Periodo	Cantidad	Monto
1	Servicio de Locador de servicio de Especialista de Ciberseguridad	Setiembre Octubre 20222	1 persona	13,000.00
				Total: S/. 13,000.00

Tabla N° 16: Presupuesto ejecutado

V. CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

- Todos los eventos detectados por las herramientas de Ciberseguridad fueron bloqueados y/o mitigados.
- No ocurrieron incidentes de Ciberseguridad en los activos informáticos que dieron soporte a las ERM 2022.
- Se mitigó un total de 7,739,175 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.

VI. ANEXOS

ANEXO (A) Informes entregados en relación al Servicio de Ethical Hacking ERM 2022

Mes	Informe
Junio	PLAN DE TRABAJO EH ERM 2022.pdf
Julio	INFORME EJECUTIVO TECNICO - SERVICIO DE ETHICAL HACKING – ONPE – ERM 2022.PDF INFORME TECNICO - SERVICIO DE ETHICAL HACKING ERM 2022 – ONPE – APLICACIONES INFORME TECNICO - SERVICIO DE ETHICAL HACKING ERM 2022 – ONPE - INFRAESTRUCTURA.PDF MATRIZ DE VULNERABILIDADES ONPE v1[R].pdf
Agosto	Informe Tecnico - Pentesting - ONPE - 31-08-2022 APLICACIONES v1.1[R].pdf Informe Tecnico - Pentesting - ONPE - 31-08-2022 INFRAESTRUCTURA v1.0[R].pdf
Noviembre	INFORME EJECUTIVO TECNICO - SERVICIO DE ETHICAL HACKING – ONPE – ERM 2022 INFORME TECNICO - SERVICIO DE ETHICAL HACKING – ONPE – INFRAESTRUCTURA INFORME TECNICO - SERVICIO DE ETHICAL HACKING – ONPE – PERSONALIZACION SEA INFORME TECNICO - SERVICIO DE ETHICAL HACKING – ONPE

Tabla N°18: Informes del servicio de Ethical Hacking ERM 2022