INFORME DE EVALUACIÓN

PLAN DE CIBERSEGURIDAD PARA EL PROCESO ELECTORAL SEGUNDA ELECCION REGIONAL 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
Segunda Elección Regional	SER 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 Segunda Elección Regional 2022 aprobado con Resolución Gerencial N° 000004-2022-GITE/ONPE (25NOV2022), 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 la Segunda Elección Regional 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 la SER 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 Noviembre – Diciembre del 2022, con un total de 12,634,748 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	$\frac{12,634,748*100\%}{12,634,748+0} = 100\%$

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
	EVALUACIÓN DE PLANES ESPECIALIZADOS Y DE ACCIÓN	Versión:	04
		Fecha de aprobación:	15/02/2018
		Página:	1 de 1

1. NOMBRE DEL PLAN - AÑO:	**Plan de Ciberseguridad SER 2022**
2. ORGANO RESPONSABLE:	**Gerencia de Informática y Tecnología Electoral**

15 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 DELPROCESO EVALUADO			12. ANALISIS CUALITATIVO		
									Nov 2022		Dic 2022							
					Inicio	Fin	Inicio	Fin	Pr	Ej	Pr	Ej	META PROGRAMADA	META EJECUTADA	% AVANCE	DESCRIPCIÓN DEL AVANCE / CUMPLIMIENTO	DIFICULTADES PRESENTADAS	MEDIDAS CORRECTIVAS
III	**PROCESOS DE SOPORTE**																	
3.2	**PROCESO: GESTIÓN DE INFRAESTRUCTURA FÍSICA Y TECNOLÓGICA**																	
3.2.4	**ACTIVIDAD: Seguridad de la Información y de la infraestructura física durante el desarrollo del Proceso Electoral**																	
1	Gestionar servicios relacionados a Ciberseguridad y monitorear las herramientas de Ciberseguridad	SGIST	Reporte	Reporte	01/11/22	31/12/22	01/11/22	31/12/22	1	1	1	1	2	2	100%	Se gestionaron los servicios de ciberseguridad como Servicio de Ethical Hacking SER 2022, IPS, Antispam Ofifice 365/checkpoint, 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 noviembre a diciembre 2022.	ninguna	ninguna
2	Coordinar reuniones semanales con los integrantes del CSIRT Electoral.	SGIST	Reporte	Reporte	01/11/22	31/12/22	04/11/22	16/12/22	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 • Fases de Ciclo de Respuesta a Incidentes de Seguridad • Preparación para manejar incidentes • Servicio de Ethical Hacking • Incident Handling Checklist • Tipos de ataques más comunes 2022 • Recomendaciones por fase	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 noviembre y diciembre 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 al Proceso Segunda Elección Regional 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	Noviembre	Diciembre	Suma de eventos
Sistema de prevención de Intrusos (IPS)	1,677		**1,677**
Antispam Office 365 / Checkpoint	1,346,601		**1,346,601**
Firewall Perimetral	1,740		**1,740**
Anti-Denegación de Servicios	0		**0**
Firewall de Aplicaciones Web Cloud	11,214,570		**11,214,570**
Firewall de Aplicaciones Web On premise	69,967		**69,967**
Antimalware (Antivirus)	193		**193**
	Total, Eventos		**12,634,748**

Tabla N° 3: Total de 12,634,748 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 1677 eventos detectados y mitigados por la herramienta IPS durante noviembre y diciembre 2022.

#	Severity	Event Name	Events Occurrences	% of Subtotal
1	Low	Default-Risky-Destination-Detection-By-Threat	1,653	99.58%
		Default-Risky-Destination-Detection-By-Endpoint	7	0.42%
		Subtotal	**1,660**	**98.99%**
2	High	Default-Risky-Destination-Detection-By-Threat	6	60.00%
		Default-Risky-Destination-Detection-By-Endpoint	4	40.00%
		Subtotal	**10**	**0.60%**
3	Medium	Default-Risky-Destination-Detection-By-Endpoint	3	42.86%
		Default-Risky-Destination-Detection-By-Threat	3	42.86%
		Local Device Event	1	14.29%
		Subtotal	**7**	**0.42%**
	Total		**1,677**	**100.00%**

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

B. Monitoreo Antimalware y Antispam Office 365:

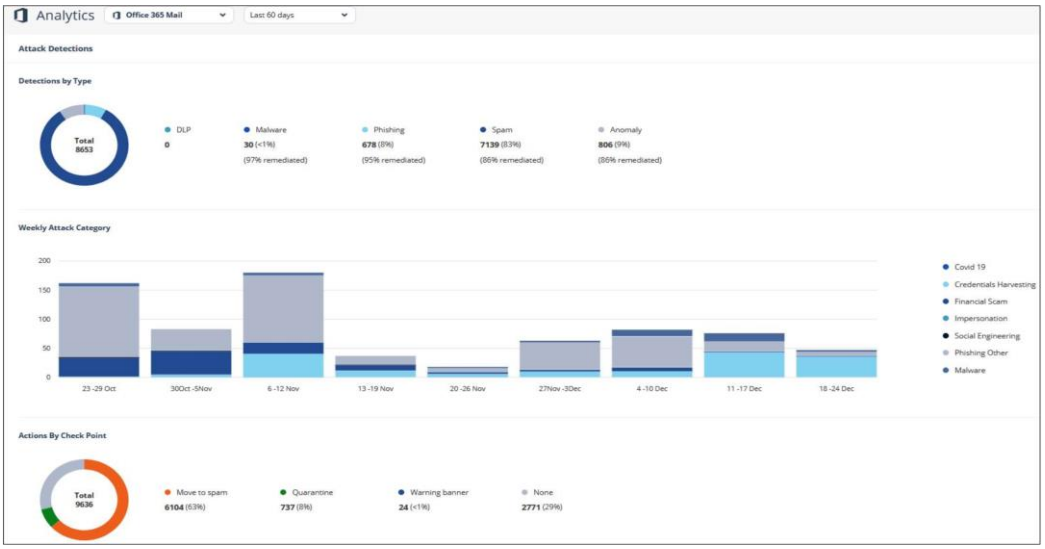
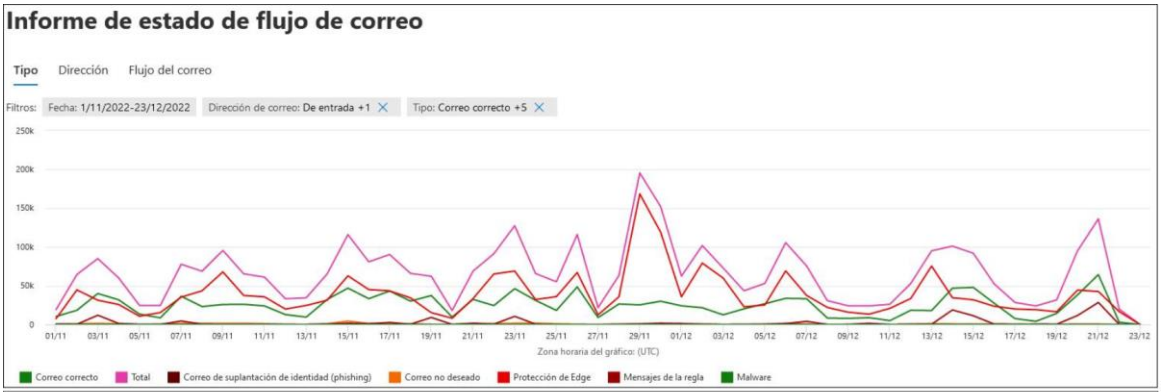


Figura N° 2: Se observa un total de 9,636 eventos detectados y mitigados por la herramienta Antispam Check Point (Harmony Email & Collaboration) durante los meses de noviembre y diciembre 2022.



Dirección	Tipo	24 horas	3 días	7 días	15 días	30 días
De entrada	Correo correcto	0	63695	121701	281599	581203
De salida	Correo correcto	0	3632	9996	30533	100604
De entrada	Correo de suplantación de id...	0	47	84	221	411
De entrada	Correo no deseado	0	774	2649	7456	19121
De salida	Correo no deseado	0	32	72	250	692
De entrada	Malware	0	0	1	54	137
De salida	Correo de suplantación de id...	0	0	1	7	15
De salida	Malware	0	0	0	0	2
De entrada	Protección de Edge	0	56610	154781	397543	1218852
De entrada	Mensajes de la regla	0	327	851	2893	5321
De salida	Protección de Edge	0	2683	4681	11117	13016
De salida	Mensajes de la regla	0	28362	40528	71508	79398

Figura N.° 3: Se observa un total de 1, 336,965 eventos detectados y mitigados por la herramienta antispam y antimalware de Microsoft 365 durante noviembre y diciembre 2022.

C. Herramienta Firewall Perimetral:

Figura N° 4: Se observa un total de 1,740 eventos detectados y mitigados por la herramienta firewall perimetral durante noviembre y diciembre 2022.

#	Severity	Event Name	Events Occurrences	% of Subtotal
1	Low	Default-Risky-Destination-Detection-By-Threat	1,714	99.59%
		Default-Risky-Destination-Detection-By-Endpoint	7	0.41%
		Subtotal	**1,721**	**98.91%**
2	Critical	Default-Compromised Host-Detection-IOC-By-Threat	8	72.73%
		Default-Compromised Host-Detection-IOC-By-Endpoint	3	27.27%
		Subtotal	**11**	**0.63%**
3	Medium	Default-Risky-Destination-Detection-By-Endpoint	3	50.00%
		Default-Risky-Destination-Detection-By-Threat	3	50.00%
		Subtotal	**6**	**0.34%**
4	High	Default-Risky-Destination-Detection-By-Endpoint	1	50.00%
		Default-Risky-Destination-Detection-By-Threat	1	50.00%
		Subtotal	**2**	**0.11%**
	Total		**1,740**	**100.00%**

Tabla Nº 5: Total 1,740 de eventos ocurridos por severidad y categoría durante noviembre y diciembre 2022.

D. Anti-Denegación de Servicios

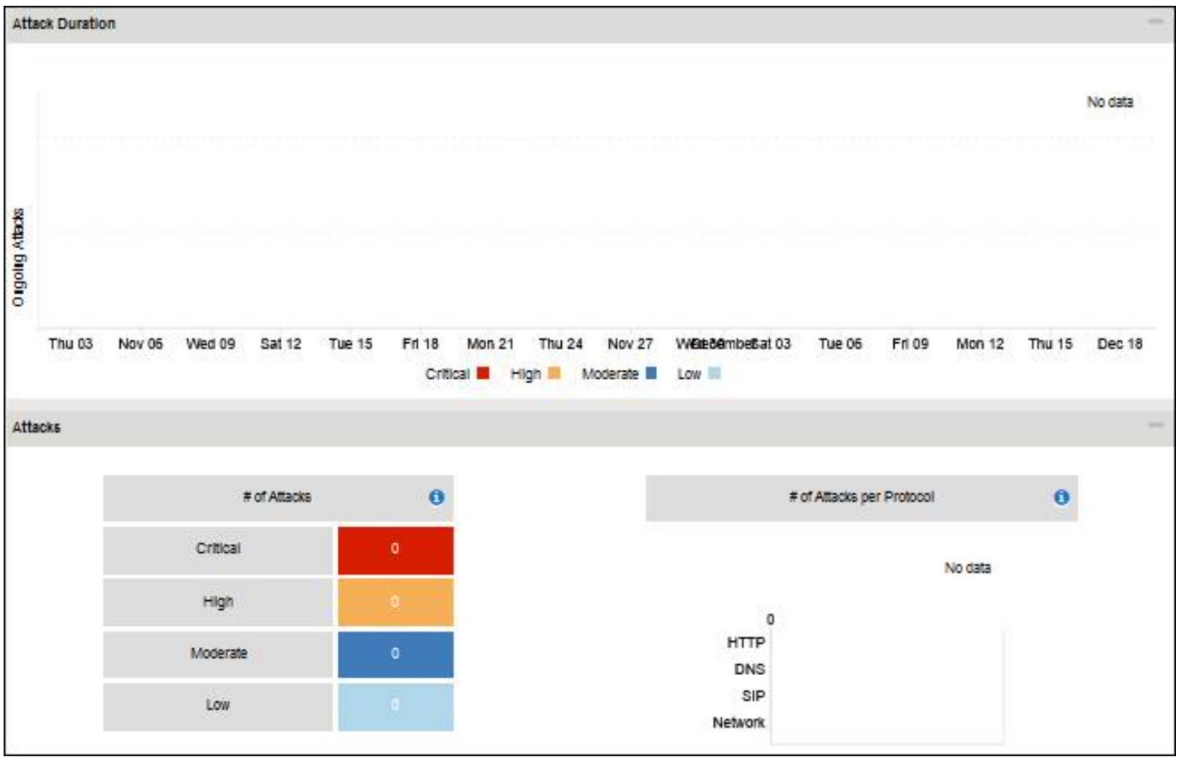


Figura N° 5: Se observa que no hubo eventos detectados en la herramienta Anti-Denegación de servicios durante los meses de noviembre y diciembre 2022.

E. Firewall de Aplicaciones Web Cloud

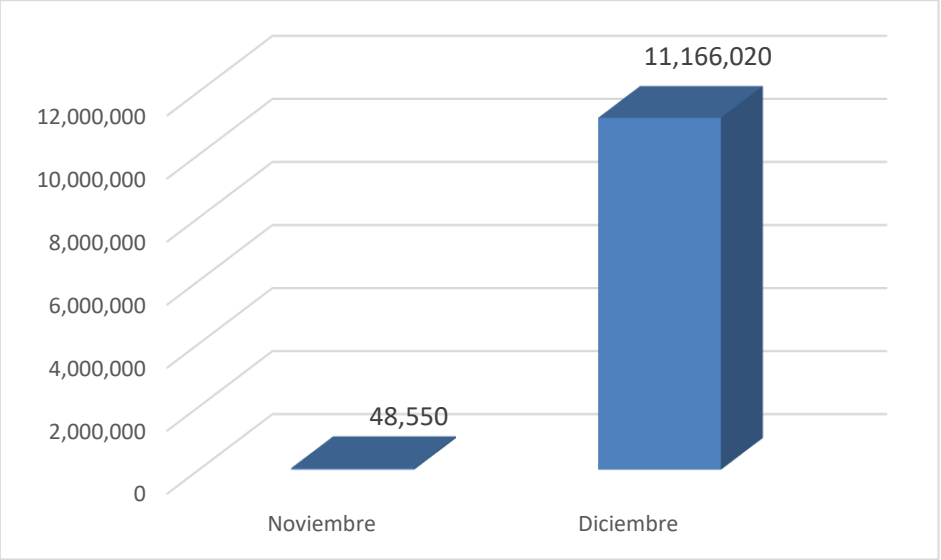


Figura N° 6: Se observa un total de 11,214,570 de eventos detectados y mitigados por la herramienta WAF para aplicaciones durante los meses de noviembre y diciembre 2022.

F. Firewall de Aplicaciones Web Onpremise

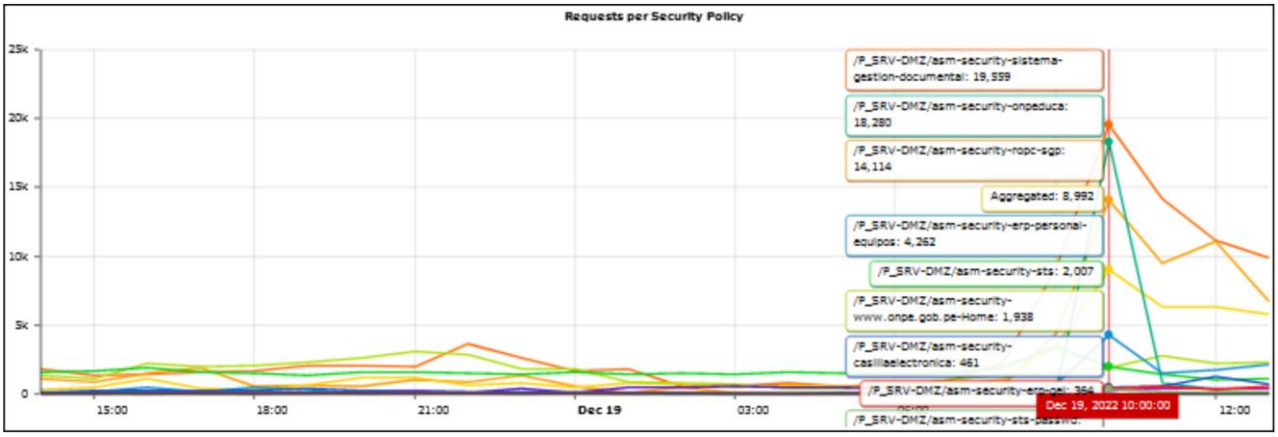


Figura N° 7: Se observa un total de 69,967 eventos detectados y mitigados por la herramienta WAF para aplicaciones On-Premise durante noviembre y diciembre 2022.

G. Antimalware (Antivirus)

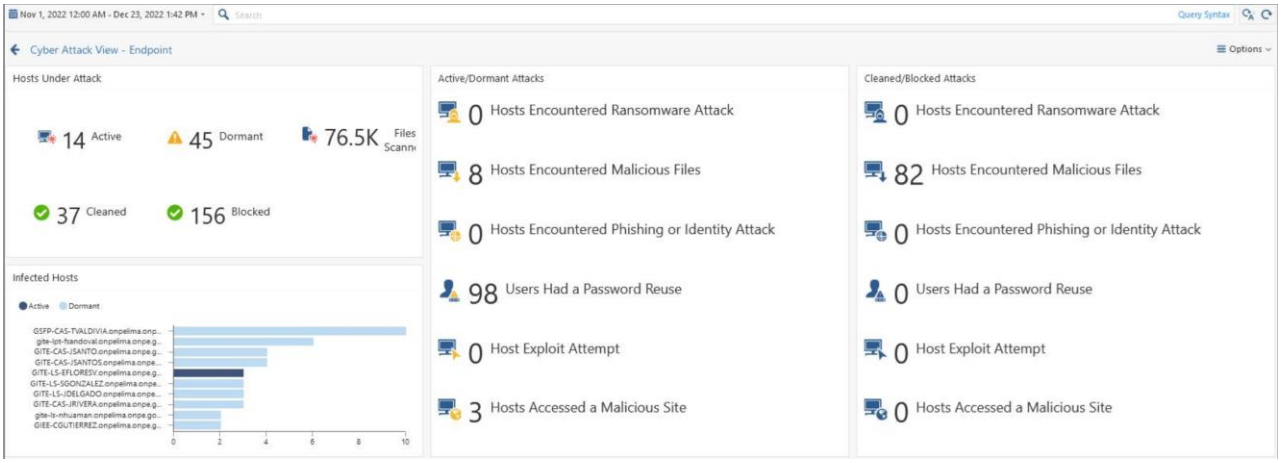


Figura N° 8: Se observa un total de 193 eventos detectados y mitigados por la herramienta Antivirus / Anti Malware – CheckPoint (Harmony Endpoint) durante noviembre y diciembre 2022.

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 al proceso de Segunda Elección Regional 2022

Así mismo, **algunos eventos detectados entre el 15NOV2022 y 20DIC2022 fueron debido a la ejecución del "Servicio Ethical Hacking SER 2022".** Tal como indica en el siguiente cronograma en el término de referencia.

ENTREGABLES	DESCRIPCIÓN	PLAZO DE ENTREGA
ENTREGABLE N° 01:	- Plan de trabajo - Compromiso de no divulgación remitido por la ONPE	Hasta los cuatro (04) días calendario siguientes de la firma del Acta de inicio
ENTREGABLE N° 02:	**Periodo: Desde el día siguiente de firmada el acta de inicio del servicio hasta el 30 de noviembre.** Contenido: - Informe técnico de infraestructura. - Informe técnico de aplicaciones, - Informe ejecutivo técnico (literal "h" del numeral 6.2). - Matriz de vulnerabilidades detectadas	Hasta los cinco (05) días calendario, posteriores a la finalización del periodo.
ENTREGABLE N° 03:	**Periodo: Desde el 01 de diciembre hasta el 20 de diciembre.** Contenido: - Informe técnico de infraestructura. - Informe técnico de aplicaciones. - Informe ejecutivo técnico (literal "h" del numeral 6.2). - Matriz de vulnerabilidades detectadas	Hasta los cinco (05) días calendario, posteriores a la finalización del periodo

Tabla N° 6: Cronograma de entregables del Servicio Ethical Hacking SER 2022

2.2. Gestionar servicios Relacionados a Ciberseguridad

Se realizó el Servicio de Ethical Hacking SER 2022 desde 15 de noviembre al 20 de diciembre de 2022, y se tienen los entregables en el Anexo (A) del presente 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).	40*
Aplicaciones	**b.7** Aplicaciones web y de escritorio.	25*

* Esta cantidad se refiere al número total de infraestructura y aplicaciones que serán puestas en producción al finalizar el periodo del servicio.

Tabla N°7: Activos del alcance del servicio de Ethical Hacking SER 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 el centro de cómputo.
7.	Desde la Red Electoral en la sede central.	Activos de Infraestructura de la Red Electoral en la sede central.

Tabla N°8: Escenarios del alcance del servicio de Ethical Hacking SER 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 repuesta a incidentes de seguridad digital fue conformado por integrantes de las distintas gerencias de GITE. A continuación, se muestra las reuniones llevadas a cabo que dieron inicio el 04NOV2022 hasta 16DIC2022; las reuniones fueron llevadas a cabo por Microsoft Teams.

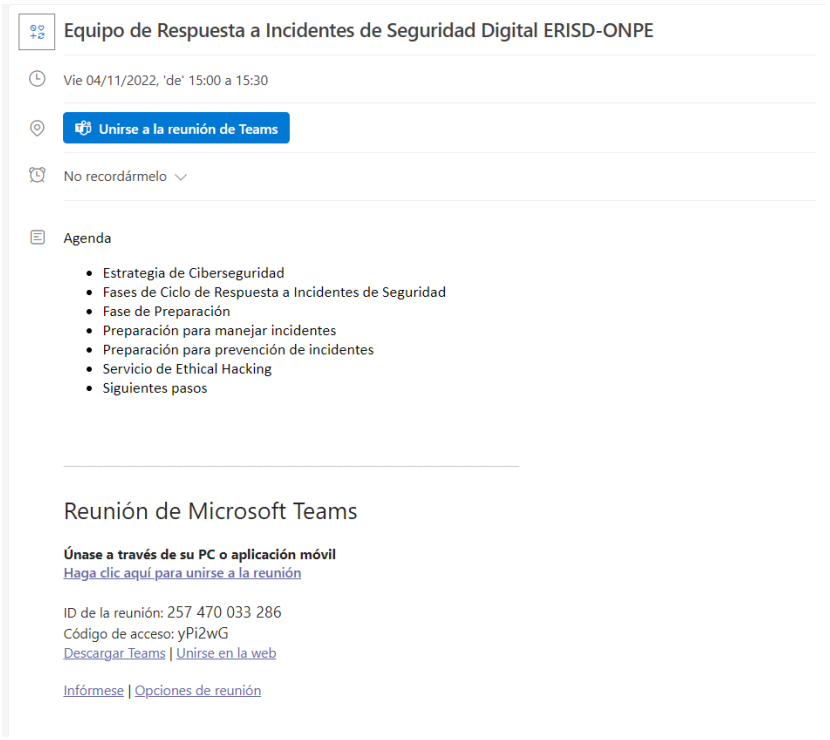


Figura 9.- Reunión ejecutada el día 04NOV2022 con el equipo ERISD-ONPE.

Las agendas que se desarrollaron se listan a continuación, cabe mencionar que se realizaron las reuniones con la frecuencia de una vez por semana.

Fecha	Titulo	Agenda
4/11/2022	Equipo de Respuesta a Incidentes de Seguridad Digital ERISD-ONPE	- Estrategia de Ciberseguridad - Fases de Ciclo de Respuesta a Incidentes de Seguridad - Fase de Preparación - Preparación para manejar incidentes - Preparación para prevención de incidentes - Servicio de Ethical Hacking - Siguientes pasos.

Fecha	Titulo	Agenda
11/11/2022	ıipo de Respuesta a Incidentes de Seguridad Digital ERISD-ONPE	- Estrategia de Ciberseguridad - Fases de Ciclo de Respuesta a Incidentes de Seguridad - Fase de Detección y Análisis - Vectores de Ataque & Signos de un Incidente - Fuentes de Precursores e Indicadores - Análisis & Documentación de un Incidente - Priorización & Notificación de un Incidente - Servicio de Ethical Hacking - Siguientes pasos.
18/11/2022	Equipo de Respuesta a Incidentes de Seguridad Digital ERISD-ONPE	- Estrategia de Ciberseguridad - Fases de Ciclo de Respuesta a Incidentes de Seguridad - Fase de Contención, Erradicación & Recuperación - Elegir una estrategia de contención - Recopilación y manejo de pruebas - Identificación de los hosts atacantes - Erradicación y Recuperación - Servicio de Ethical Hacking - Siguientes pasos.
25/11/2022	Equipo de Respuesta a Incidentes de Seguridad Digital ERISD-ONPE	- Estrategia de Ciberseguridad - Fases de Ciclo de Respuesta a Incidentes de Seguridad - Fase de Post Incidente Actividades - Lecciones Aprendidas - Uso de datos de incidentes recopilados - Retención de evidencia - Incident Handling Checklist - Recomendaciones - Servicio de Ethical Hacking - Siguientes pasos.
2/12/2022	Equipo de Respuesta a Incidentes de Seguridad Digital ERISD-ONPE	- Estrategia de Ciberseguridad - Tipos de Ataques más comunes 2022 - Resumen de Fases de Ciclo de respuestas a Incidentes - Recomendaciones por fase - Servicio de Ethical Hacking SER 2022 - Siguientes pasos.
16/12/2022	Equipo de Respuesta a Incidentes de Seguridad Digital ERISD-ONPE	- Estrategia de Ciberseguridad - Tipos de Ataques más comunes - Riesgos de Ciberseguridad - Inventario de Activos - Servicio de Ethical Hacking SER 2022 (2do entregable) - Siguientes pasos

Tabla N°9: Listado de agenda de reuniones realizadas.

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 SER 2022.

3.2. Problemas identificados y medidas correctivas adoptadas

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

IV. EJECUCIÓN DEL PRESUPUESTO

El presupuesto en el incurre para la ejecución del "PLAN DE CIBERSEGURIDAD SER 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 SER 2022	Periodo	Cantidad	Monto
1	Servicio de Locador de servicio de Especialista de Ciberseguridad	Noviembre Diciembre 20222	1 persona	13,000.00
				Total: S/. 13,000.00

Tabla N° 10: 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 SER 2022.

- Se mitigó un total de 12,634,748 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 SER 2022, cabe mencionar que en el 2do entregable se realizo el informe de todos los activos de infraestructura por eso en el 3er entregable solo se abarco el informe de aplicaciones.

Entregable	Informe
1er Entregable	ACTA DE INICIO.pdf TDR SERVICIO DE ETHICAL HACKING - SER2022_V00.pdf
2do Entregable	Informe Tecnico - Pentesting - ONPE - 30-11-2022 APLICACIONES v1.0[R].pdf Informe Tecnico - Pentesting - ONPE - 30-11-2022 INFRAESTRUCTURA v1.0[R].pdf Informe Ejecutivo Tecnico - ONPE - 30-11-2022 ETHICAL HACKING SER2022 v1.0[R].pdf MATRIZ DE VULNERABILIDADES ONPE 30-11-2022 v1.0[R].pdf
3er Entregable	Informe Ejecutivo Tecnico - ONPE - 20-12-2022 ETHICAL HACKING SER2022 v1.0[R].pdf Informe Tecnico - Pentesting - ONPE - 20-12-2022 APLICACIONES v1.0[R].pdf MATRIZ DE VULNERABILIDADES ONPE 20-12-2022 v1.0[R].pdf

Tabla N°11: Informes del servicio de Ethical Hacking SER 2022