"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año del Fortalecimiento de la Soberanía Nacional"
"Año del Bicentenario del Congreso de la República del Perú"

RESOLUCION GERENCIAL N° 000004-2022-GITE/ONPE

Lima, 25 de Noviembre del 2022

VISTOS: La Resolución Jefatural N° 004287-2022-JN/ONPE, de fecha 10 de noviembre de 2022;

CONSIDERANDOS:

Que, con Memorando N° 006008-2022-GITE/ONPE de fecha 09 de noviembre del 2022, la Gerencia de Informática y Tecnología Electoral (en adelante GITE) remitió a la Gerencia de Planeamiento y Presupuesto, la propuesta de *"Plan de Ciberseguridad para el proceso electoral Segunda Elección Regional 2022", versión 00 (Plan Especializado),* para su revisión y conformidad;

Que, con Memorando N° 005073-2022-GPP/ONPE, de fecha 24 de noviembre del 2022, la GPP brindó opinión favorable a la propuesta del plan, y trasladó a la GITE el INFORME N° 000533-2022-SGPL-GPP/ONPE, mediante el cual, la Subgerencia de Planeamiento (SGP), recomienda continuar con el trámite de aprobación *"Plan de Ciberseguridad para el proceso electoral Segunda Elección Regional 2022", versión 00*. Asimismo, en el referido documento, la SGP comunica que, con Memorando N° 000100-2022-SGPR-GPP/ONPE; la Sub Gerencia de Presupuesto (SGPR) señala que el referido plan, cuenta con los recursos necesarios, por la suma de S/ 13,000.00, en marco de la Segunda Elección Regional - SER 2022.

Que, conforme a lo dispuesto en los ítems 9) y 10) del numeral 6.1.2 del Procedimiento "Formulación, modificación, monitoreo y evaluación de los Planes Institucionales de la ONPE", con código PR01-GPP/PLAN - versión 00", la aprobación de los Planes de Acción se realiza mediante Resolución Gerencial, del órgano formulador, debiendo ponerse a conocimiento de la Jefatura Nacional y la Gerencia de Planeamiento y Presupuesto y de los demás órganos de la institución;

Que, debido a lo señalado, resulta pertinente la emisión de la Resolución Gerencial que apruebe el *"Plan de Ciberseguridad para el proceso electoral Segunda Elección Regional 2022", versión 00 (Plan Especializado);*

De conformidad con lo dispuesto en el literal t) del Artículo 83° del Reglamento de Organización y Funciones de la ONPE aprobado mediante Resolución Jefatural N° 063-2014-J/ONPE, modificado mediante Resolución Jefatural N° 155-2020-JN/ONPE

SE RESUELVE:

Artículo Primero. - Aprobar el *"Plan de Ciberseguridad para el proceso electoral Segunda Elección Regional 2022", versión 00 (Plan Especializado)*; documento que como anexo forma parte integrante de la presente resolución.

Artículo Segundo. - Disponer que el cumplimiento, supervisión y evaluación del *"Plan de Ciberseguridad para el proceso electoral Segunda Elección Regional 2022", versión 00 (Plan Especializado)* sea de responsabilidad de la Sub Gerencia de Infraestructura y Seguridad Tecnológica.

Artículo Tercero. - Disponer la remisión de la copia de la presente resolución y del plan, a todos los órganos de la institución.

Artículo Cuarto. - Disponer la publicación de la presente resolución y su anexo en el Portal Institucional www.onpe.gob.pe dentro del plazo de tres (3) días de su emisión.

Regístrese, comuníquese y cúmplase.

DOCUMENTO FIRMADO DIGITALMENTE
ROBERTO CARLOS MONTENEGRO VEGA
Gerente de la Gerencia de Informática y Tecnología Electoral
Oficina Nacional de Procesos Electorales

PLAN DE CIBERSEGURIDAD PARA EL PROCESO ELECTORAL SEGUNDA ELECCION REGIONAL 2022

(Plan Especializado)

Gerencia de Informática y Tecnología Electoral

LIMA, NOVIEMBRE 2022

VERSIÓN 00

Firmado digitalmente por MONTENEGRO VEGA Roberto Carlos FAU 20291973851 soft
Motivo: Doy V° B°
Fecha: 25.11.2022 21:29:12 -05:00

Firmado digitalmente por SAMAME BLAS Jose Edilberto FAU 20291973851 soft
Motivo: Doy V° B°
Fecha: 25.11.2022 15:55:06 -05:00

Firmado digitalmente por POLO PALACIOS Miguel Angel FAU 20291973851 soft
Motivo: Soy el autor del documento
Fecha: 25.11.2022 15:49:25 -05:00

INDICE

ABREVIATURAS

NOMBRE	ABREVIATURA
Comando Conjunto de las Fuerzas Armadas	CCFFAA
Comando Operacional de Ciberdefensa	COCIB
Cloud Access Security Broker	CASB
Dirección de Inteligencia de la PNP	DIRIN
Dirección Nacional de Inteligencia	DINI
División de Investigaciones de Delitos de Alta Tecnología…	DIVINDAT
Equipo de Respuesta ante Incidentes de Ciberseguridad	CSIRT
Firewall de aplicaciones web	WAF
Gerencia de Gestión Electoral	GGE
Gerencia de Información y Educación Electoral	GIEE
Gerencia de Informática y Tecnología Electoral	GITE
Gerencia de Organización Electoral y Coordinación Regional	GOECOR
Gestión de dispositivos móviles	MDM
Gestión del Riesgo de Desastres	GRD
Instituto Nacional de Tecnología y Estándar	NIST
Jefatura Nacional	JN
Jurado Electoral Especial	JEE
Jurado Nacional de Elecciones	JNE
Lista de Control de Acceso	ACL
Mecanismo de Servicios de Identidad	ISE
Ministerio Público	MP
Oficina Descentralizada de Procesos Electorales	ODPE
Oficina Nacional de Procesos Electorales	ONPE
Presidencia de Concejo de Ministros	PCM
Policía Nacional del Perú	PNP
Red de Distribución de Contenidos	CDN
Registro Nacional de Identificación y Estado Civil	RENIEC
Secretaría General	SG
Secretaría de Gobierno Digital (COMITÉ DE GOBIERNO Y TRANSFORMACION DIGITAL – GTD)	SEGDI
Sistema de Correlación de Eventos de Seguridad	SIEM
Sistema de Prevención de Intrusos	IPS
Subgerencia de Operaciones Electorales	SGOE
Equipos de Respuesta de Incidentes de Seguridad Digital	ERISD

I. INTRODUCCIÓN

Conforme al artículo N°1 de la Ley N° 26487, Ley Orgánica de la Oficina Nacional de Procesos Electorales (ONPE), establece que la ONPE es un organismo autónomo que cuenta con personería jurídica de derecho público interno y goza de atribuciones en materia técnica, administrativa, económica y financiera, siendo la autoridad máxima en la organización y ejecución de los procesos electorales, de referéndum y otros tipos de consulta popular a su cargo.

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.

Según la Resolución Jefatural N° 004287-2022-JN/ONPE (10NOV2022) se aprueba, el Plan Operativo Electoral Segunda Elección Regional 2022 versión 01. Así mismo este documento describe en forma detallada el Plan de Ciberseguridad a desarrollarse en época electoral, con el fin garantizar, que la información que se encuentra en el ciberespacio de la ONPE mantenga las siguientes características de seguridad:

- ***Confidencialidad:*** Garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- ***Integridad:*** Salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.
- ***Disponibilidad:*** Garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
- ***Autenticidad:*** Asegurar que la validez de la información en tiempo forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- ***Auditabilidad:*** Definir que todos los eventos de un sistema puedan ser registrados para su control posterior.
- ***Protección a la duplicación:*** Asegurar que una transacción sólo se realice una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- ***No repudio:*** Evitar que una entidad que haya enviado o recibido información o intercambiados datos alegue ante terceros que no los envió o no los recibió.
- ***Legalidad:*** Cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- ***Confiabilidad de la Información:*** Que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

II. MARCO LEGAL

- Constitución Política del Perú.
- Ley N.º 26487, Ley Orgánica de la Oficina Nacional de Procesos Electorales (ONPE).
- Ley N.º 26859, Ley Orgánica de Elecciones y sus modificaciones.
- Ley N.º 28094, Ley de Organizaciones Políticas y sus modificaciones.
- Ley N.º 29603, Ley que autoriza a la ONPE a emitir las normas reglamentarias para la implementación gradual y progresiva del voto electrónico.
- Ley N.º 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres – SINAGERD.
- Ley N.º 30225, Ley de Contrataciones del Estado y sus modificaciones.
- Ley N.º 30998, Ley que modifica a la Ley 28094, Ley de Organizaciones Políticas, para promover la participación política y la democracia en las Organizaciones Políticas.
- Ley N.º 30999, Ley de Ciberdefensa, el cual establece la respuesta a incidentes relacionados con activos críticos nacionales.
- Decreto Supremo N.º 106-2017-PCM “Decreto Supremo que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales (ACN).
- Decreto Supremo N.º 115 – 2022 - PCM, que aprueba el Plan Nacional de Gestión de Riesgos de Desastres – PLANAGERD 2022 – 2030.
- Decreto Legislativo N.º 1095, Decreto Legislativo que establece Reglas de empleo y Uso de la Fuerza por parte de las Fuerzas Armadas en el Territorio Nacional.
- Decreto Legislativo N.º 1412, define, que la Seguridad Digital es el estado de confianza en el entorno digital, que resulta de la gestión y aplicación de un conjunto de medidas proactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.
- Resolución Ministerial N.º 360-2009-PCM, de fecha 19 de agosto de 2009, se crea el grupo de trabajo permanente, denominado

Coordinadora de Respuesta de Emergencias en Redes Teleinformáticas de la Administración Pública del Perú (Pe-CERT), con el objetivo, entre otros, de promover la coordinación entre las entidades de la administración de redes informáticas de la Administración Pública Nacional, para la prevención, detección, manejo, recopilación de información y desarrollo de soluciones para los incidentes de seguridad digital.

- Resolución Ministerial N.º 004-2016-PCM (Pub. 14ENE2016) que aprueba la Norma Técnica Peruana "NTP ISO/IEC 27001:2014. Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Suprema N.º 016-DE/CCFFAA-D3-IE, Reglamento de servicio en guarnición para las Fuerzas Armadas y Policía Nacional del Perú y su modificatoria, regula las normas y procedimientos de los Institutos de las Fuerzas Armadas y de la Policía Nacional del Perú para el servicio en la Guarnición, la Disciplina, Ley y Orden de sus miembros y la seguridad interna en la jurisdicción de las guarniciones.
- Resolución de la Fiscalía de la Nación N.° 1503-2020-MP-FN, que crea la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional, la misma que dependerá administrativa y funcionalmente de la Fiscalía de la Nación.
- Resolución Jefatural N.º 000093-2017-J/ONPE, que aprueba la Directiva Lineamientos de Seguridad de la Información, con Código DI04-GGC/GC, Versión: 00.
- Resolución Jefatural N.º 000094-2017-J/ONPE, que aprueba la declaración documentada de la Política de Seguridad de la Información de la Oficina Nacional de procesos Electorales, Código: OD10-GGC/GC-Versión 00.
- Resolución Jefatural N.º 000419-2020-JN/ONPE (19NOV2020), que aprueba la Directiva Formulación, Reprogramación, Monitoreo y Evaluación de los Planes Institucionales de la ONPE.
- Resolución Jefatural N.º 000169-2020-JN/ONPE (07AGO2020), que aprueba el" Plan de Contingencia 2020 – 2022" versión 00 de la Oficina Nacional de Procesos Electorales.
- Resolución Jefatural N.º 000172 - 2020-JN/ONPE (10AGO2020), que aprueba el" Plan de Continuidad Operativa 2020 – 2022" versión 00 de la Oficina Nacional de Procesos Electorales.
- Resolución Jefatural N.º 000173-2020-JN/ONPE (10AGO2020), que aprueba el" Plan de Prevención y Reducción del riesgo de Desastres 2020 – 2022" versión 00 de la Oficina Nacional de Procesos

Electorales.

- Resolución Jefatural N.º 000902-2021-JN/ONPE(30SET2021), que aprueba la adecuación el Reglamento de Organización y Funciones de la Oficina Nacional de Procesos Electorales aprobado por Resolución Jefatural N.º 063-2014-J/ONPE y sus modificatorias.

- Reglamento de Organización y Funciones de la Oficina Nacional de Procesos Electorales, artículo N.º 82, una de las funciones de la Gerencia de Informática y Tecnología Electoral, es “realizar la innovación hacia servicios públicos electorales seguros con énfasis en las políticas de Gobierno Abierto en el marco de la Infraestructura Oficial de Firma Electrónica”.

- Resolución de Gerencia General N.º 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.

- Resolución Jefatural N.º 002108-2022-JN/ONPE (01JUN2022), que aprueba el Plan Estratégico Institucional para el período 2020-2025 de la ONPE.

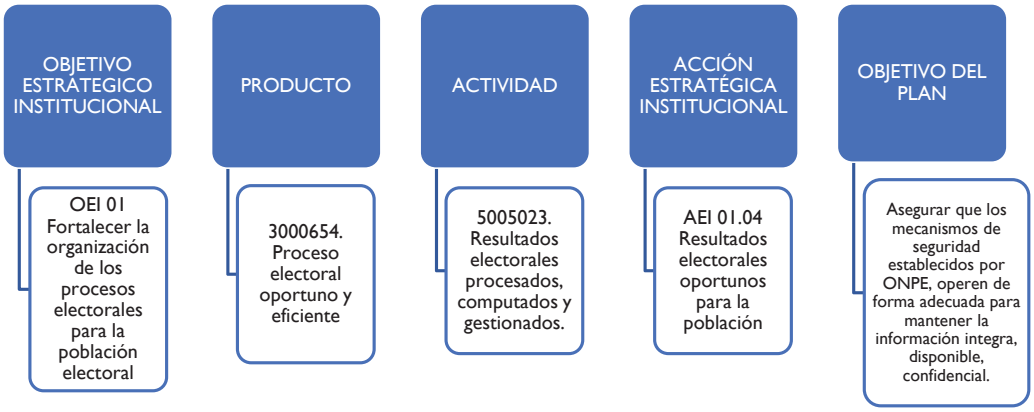
- Resolución Jefatural N.º 003733-2022-JN/ONPE (19OCT2022), que aprueba el Plan Operativo Electoral Segunda Elección Regional 2022”, Versión 00.

- Resolución Jefatural N.° 004287-2022-JC/ONPE (10NOV2022) se aprueba, el Plan Operativo Electoral Segunda Elección Regional 2022 versión 01.
- Documentos del Sistema de Gestión de la Calidad: Manual de Calidad, directivas, procedimientos, instructivos y formatos vinculados a procesos electorales.

III. MARCO ESTRATÉGICO

3.1 Alineación de Objetivos

El objetivo de este Plan esta alineado a los objetivos estratégicos institucionales, señalados en el PEI 2020-2025, que determinan el accionar de la institución, asimismo estos objetivos, se encuentran alineados a los productos del Programa Presupuestal N° 0125: “Mejora de la Eficiencia de los Procesos Electorales e Incremento de la Participación Política de la Ciudadanía”.



IV. MARCO CONCEPTUAL

4.1 Aspectos Generales

El servicio de Ciberseguridad permitirá gestionar los riesgos, monitorear y proteger los servicios y la infraestructura crítica gestionada por los procesos de la Gerencia de Informática y Tecnología Electoral de la ONPE, ante cualquier ciber amenaza y ciber riesgo que ponga en peligro la integridad, confidencialidad y disponibilidad de la información, por medio de la implementación de los diversos componentes de Ciberseguridad que se describen en el presente documento.

Antes y durante el periodo de la actividad electoral, los sistemas de información pueden ser víctimas de amenazas cibernéticas, tales como aquellas destinadas a la alteración de información obtenida, modificación de la página web de la entidad o fuga de información confidencial. Para evitar ello, es recomendable implementar diversas acciones de Ciberseguridad.

Para dar servicios electorales seguros se requiere, la implementación de diversas medidas que garanticen la seguridad de la información durante la ejecución de las diversas actividades electorales.

Cabe mencionar que este Plan este alienado a cumplir con la norma ISO/IEC 27001:2022 Gestión de Seguridad de la Información. Así mismo, también como buena práctica guiamos con la norma ISO/IEC 27032 “Guía de Ciberseguridad”, la Ciberseguridad, está enfocada al aseguramiento de la información digital, redes de datos, Internet y protección de la infraestructura crítica de información digital.

Con el objetivo de ejecutar acciones que permitan garantizar la confidencialidad, integridad y disponibilidad de la información digital, se toma en consideración el Marco de Ciberseguridad NIST (*National Institute of Standards and Technology*). El marco de Ciberseguridad NIST, inició con la Orden Ejecutiva N° 13636 de los Estados Unidos, publicada el 12 de febrero de 2013, la mencionada orden introdujo esfuerzos para compartir información sobre amenazas de ciberseguridad y construir un conjunto de enfoques actuales y exitosos para reducir riesgos en infraestructura crítica. Las funciones del marco de Ciberseguridad NIST son las siguientes:

Figura 1: Marco de Ciberseguridad NIST[2]

[2] https://www.nist.gov/cyberframework
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271es.pdf

En ese sentido, la Sub Gerencia de Infraestructura y Seguridad Tecnológica, propone como estrategia de Ciberseguridad el marco NIST (National Institute of Standards and Technology), para cumplir con lo establecido en el ROF de la entidad.

Cabe mencionar, que la estrategia de Ciberseguridad considera las herramientas necesarias que se encuentran dentro del alcance funcional de la ONPE tanto en época electoral, la normatividad que la rige; y son las siguientes:

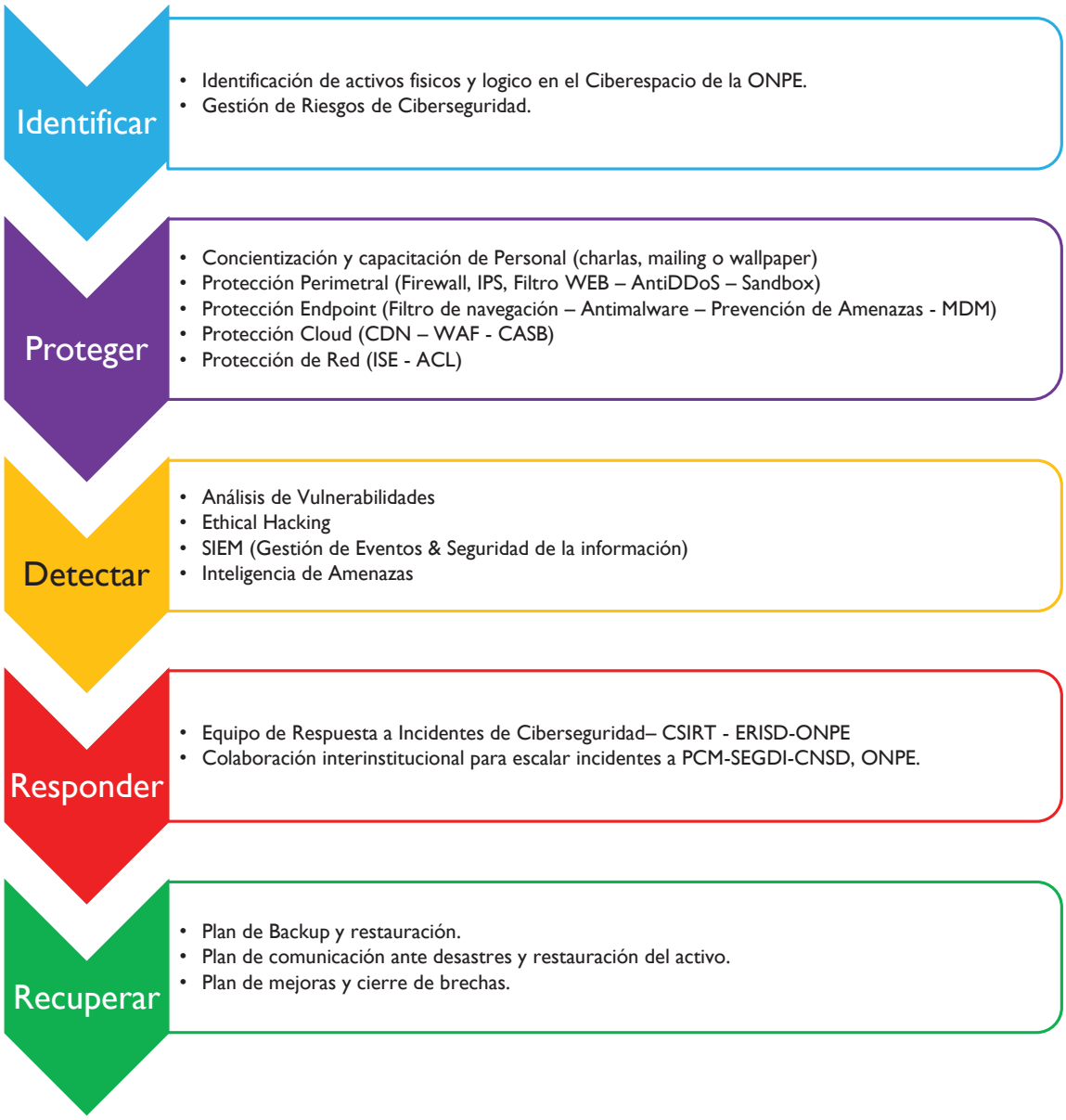


Figura 1: Componentes de la Estrategia de Ciberseguridad para la ONPE

4.2. Alcance general de las fases para época electoral.

Cabe indicar que cada fase posee servicios de Ciberseguridad que se requieren para garantizarla seguridad de los activos informáticos que se encuentran en el ciberespacio de la ONPE. El alcance de cada servicio es el siguiente:

Fase	Detalles del servicio
Identificación	**Identificación de activos en el Ciberespacio de la ONPE** Identificar usuarios, medios de comunicación digital, sistemas informáticos, software, así como hardware de procesamiento, almacenamiento y comunicaciones.
	Gestión de Riesgos de Ciberseguridad **Evaluación de Riesgos a los activos del Ciberespacio de la ONPE** Evaluación de los riesgos encontrados de forma cualitativa. **Estrategia de Mitigación** Procedimientos para evitar, reducir, absorber, mitigar y/o transformar cada riesgo encontrado. **Ejecución de Estrategias** Ejecución de las estrategias de mitigación en cada riesgo encontrado. **Análisis de Brechas** Medición del nivel de madurez actual de los controles de ciberseguridad y elaboración de un plan para aplicar controles adecuados con el objetivo de alcanzar el estado deseado. **Control del Riesgo** Medición de la efectividad de la estrategia de mitigación.
Protección	**Concientización y capacitación** Todos los colaboradores, terceros y proveedores deben conocer y estar familiarizados con las políticas de Ciberseguridad de la ONPE.
	Protección perimetral. Solución Firewall de siguiente generación, con funcionalidad de sandboxing para mitigar toda filtración de malware de día cero y malware avanzado desde la Internet a la red Interna. Solución Firewall de Aplicaciones Web para mitigar todo comportamiento malicioso en las aplicaciones y sistemas informáticos de la entidad publicados en la red interna, así como en Internet.
	Protección Endpoint Solución que permite proteger a los equipos de usuario final y servidores ante amenazas avanzadas como programa maligno, spyware, botnets, entre otros.
	Protección Cloud En el contexto de pandemia muchos colaboradores se encuentran realizando trabajo remoto por lo que se recomienda implementar una protección perimetral de tipo CASB para proteger a la información sensible que se encuentra en plataformas colaborativas como Office 365.
	Protección de Red Herramientas que permiten conectarse a la red de forma lógica, solo a dispositivos autorizados (Network Access Control).

Detección	**Análisis de Vulnerabilidades.** Herramienta para detectar vulnerabilidades y hacer seguimiento a su mitigación con el fin cerrar toda brecha de seguridad.
	Ethical Hacking. Servicio realizado por un tercero, que evalúe el estado de la seguridad en los activos informáticos internos y públicos de la ONPE.
	SIEM. Sistema para correlacionar de eventos que mediante casos de uso puede detectar anomalías y eventos inusuales que ocurren en la red, sistemas informáticos y activos de cómputo.
	Inteligencia de amenazas Sistema automatizado que permite detectar de forma temprana fuga de información, credenciales comprometidas, ataques a la marca, así como ataques a la infraestructura y sistemas informáticos de la entidad.
Respuesta	**Equipo de Respuesta a Incidentes de Ciberseguridad ERISD-ONPE** Mantener la comunicación con el equipo conformado por miembros de la ONPE del sistema electoral peruano, sus proveedores ISP, PCM, para la coordinación, apoyo y mitigación de incidentes que atenten contra los activos informáticos que conforman el sistema electoral del Perú.
	Colaboración interinstitucional para escalar incidentes a PCM-SEGDI. Es preciso escalar toda amenaza que se materializa en Incidente a las autoridades pertinentes para dejar un registro e iniciar procesos legales contra los responsables del daño ocasionado.
Recuperación	**Plan de Backup para restauración** Es preciso mantener el plan de backups actual para restaurar cualquier servicio en caso ocurra un incidente.
	Plan de comunicación ante desastres y restauración del activo Es necesario mantener un plan de comunicación y contactos a quienes llamar durante un incidente. Además, se requiere realizar pruebas de restauración con el objetivo de medir tiempos para levantar un servicio en caso ocurra un incidente
	Plan de mejoras y cierre de brechas Se requiere establecer una bitácora con lecciones aprendidas del incidente y a partir de la lección aprendida, realizar una mejora en el control de seguridad para evitar que el incidente vuelva a ocurrir.

4.3. Estrategia en época electoral

Para dar respuesta a los incidentes de seguridad digital que ocurran, se conforma un Equipo de Respuesta ante Incidentes de Seguridad Digital de la Oficina Nacional de Procesos Electorales.

Objetivo:

Disponer de una coordinación eficiente y centralizada para todo lo relacionado con la Ciberseguridad (Seguridad Digital) dentro del Sistema Electoral del Perú, el cual permitirá la gestión proactiva de incidentes, así como monitorear y

reaccionar de forma estandarizada; con la finalidad de proteger los servicios y la infraestructura crítica y cualquier activo de información que soporte el correcto funcionamiento de todas las actividades involucradas en los Procesos Electorales, ante cualquier ciber amenaza que ponga en peligro la integridad, confidencialidad y la disponibilidad de la información en dichos procesos.

Alcance:

Todos los incidentes de Seguridad Digital relacionados al Sistema Electoral en relación con los servicios y la infraestructura crítica gestionada por los integrantes e interesados del Sistema Electoral Peruano.

Comunidad objetivo:

El Ciberespacio de la ONPE.

Interesados:

Dentro de los principales interesados se lista a los siguientes:
- ONPE
- PCM-SEGDI-Centro Nacional de Seguridad Digital.

Equipo de Respuestas ante Incidentes de Seguridad Digital de la Oficina Nacional de Procesos Electorales - ERISD-ONPE

El CSIRT (Computer Security Incident Response Team) es un ***Equipo de Respuesta a incidentes de Seguridad Digital*** de la **Oficina Nacional de Procesos Electorales**. Se trata de un grupo de expertos responsables del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad digital en los sistemas de información.

La ONPE, designará a un equipo de especialistas, capacitados en Seguridad Digital, que darán respuesta a incidentes de seguridad digital. Este equipo designado realizará el monitoreo de incidentes y amenazas desde sus respectivas áreas. El monitoreo en horario 24x7 iniciará una semana antes de las elecciones y finalizará una semana después de realizarse las elecciones respectivas, posteriormente el monitoreo se realizará en horario de oficina.

Para la gestión de amenazas e incidentes, se debe utilizar herramientas de monitoreo, dentro del proceso de gestión de incidentes de Seguridad Digital, así mismo, los integrantes del Equipo de Respuestas ante Incidentes de Seguridad Digital de la Oficina Nacional de Procesos Electorales - ERISD-ONPE, realizaran de forma continua una Inteligencia de amenazas cibernéticas y análisis de vulnerabilidades.

El Equipo de Respuestas ante Incidentes de Seguridad Digital de la Oficina Nacional de Procesos Electorales - ERISD-ONPE, por medio del conjunto de acciones que realizará cada miembro, realizará la detección e identificación de

incidentes y amenazas en el ciberespacio del Sistema Electoral, que pongan en riesgo la integridad, confidencialidad y disponibilidad de los activos informáticos que soportan el proceso electoral.

El Equipo de Respuestas ante Incidentes de Seguridad Digital de la Oficina Nacional de Procesos Electorales - ERISD-ONPE debe generar informes con la detección de amenazas e incidentes ocurridos, una semana antes de las elecciones y finalizará una semana después de realizarse las elecciones. Los integrantes del Equipo de Respuestas ante Incidentes de Seguridad Digital de la Oficina Nacional de Procesos Electorales - ERISD-ONPE, en el marco de las funciones que desempeñarán y la información a la que tendrán acceso, deben firmar un acuerdo de confidencialidad, para mantener la reserva de dichos informes y toda la información que se procese.

Cabe mencionar, que cada actividad de monitoreo realizada, debe estar orientado a proteger la Seguridad (Integridad, Confidencialidad, y Disponibilidad) en las redes, activos críticos y servicios publicados a los ciudadanos en el marco de la actividad electoral, así mismo se debe tener las capacidades para detectar cualquier actividad maliciosa, por medio de herramientas o sensores instalados en distintas plataformas con el objetivo de informar, gestionar y responder ante distintas alarmas en coordinación con los integrantes del Equipo de Respuestas ante Incidentes de Seguridad Digital.

Conformación del ERISD-ONPE

El Equipo de Respuestas ante Incidentes de Seguridad Digital estará conformado por las miembros de la Gerencia de Informática y Tecnología Electoral. Así mismo, el siguiente gráfico muestra a las Gerencias y Sub Gerencias que conforman el ERISD-ONPE, los cuales designarán personal con experiencia en Ciberseguridad para poder gestionar incidentes de Seguridad Digital. Además, el gráfico muestra la cooperación interinstitucional entre las entidades para obtener fuentes de conocimiento de amenazas que puedan atentar contra la seguridad digital de los servicios durante el periodo electoral.

"Los miembros del CSIRT se capacitan usando la Plataforma de Centro de Conocimiento Digital, integrante de la Plataforma Nacional de Talento Digital"
https://auladigital.cnsd.gob.pe

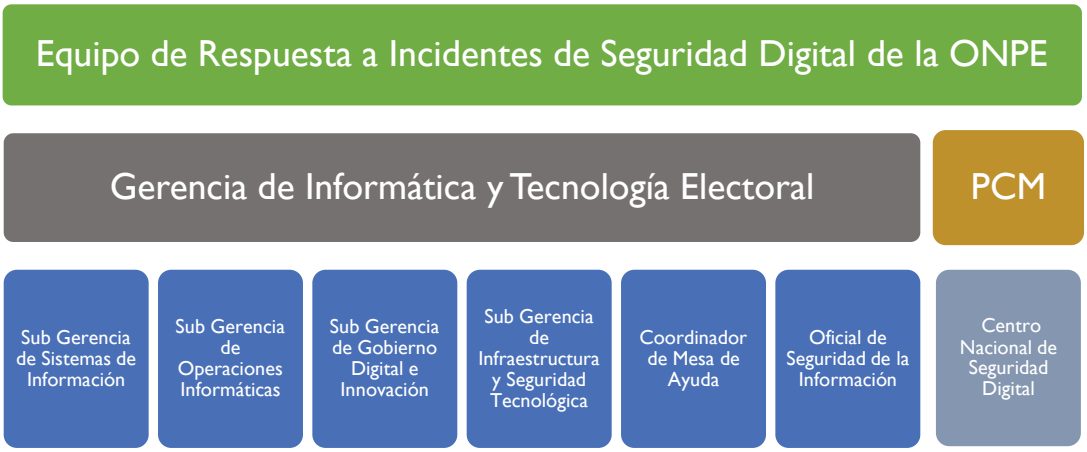


Figura 1: Equipo de Respuestas ante Incidentes de Seguridad Digital de la Oficina Nacional de Procesos Electorales - ERISD-ONPE

Servicios del ERISD-ONPE

Conforme al Marco de servicios del equipo de respuesta a incidentes de seguridad informática (CSIRT), propuesto por el Foro de equipos de seguridady respuesta a incidentes, ***FIRST***[3]. El ERISD-ONPE debe estar conformado por las siguientes áreas de servicio para una completa gestión del incidente de seguridad digital

Figura 2: Áreas de servicio del ERISD-ONPE

[3] FIRST 2019. Marco de servicios FIRST CSIRT, https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

Roles ERISD-ONPE

Un integrante del ERISD-ONPE puede desempeñar más de un rol en las áreas de servicio, como buena práctica se menciona debajo en los siguientes roles.

Líder de ERISD-ONPE

- Representante del ERISD de la ONPE

Gestor de eventos de seguridad digital

- Un recurso en ONPE por el Sistema Electoral.
- Será responsable de identificar los incidentes de seguridad digital, basado en Inteligencia de amenazas cibernéticas, correlación y análisis de los eventos de seguridad provenientes de los sensores de seguridad y fuentes de datos contextuales.
- Debe informar al ERISD - ONPE ante cualquier incidente o amenaza que ponga en peligro el normal desarrollo del proceso electoral y, en el marco de los procedimientos de respuesta a incidentes, debe coordinar con las entidades pertinentes, y de corresponder escalar el incidente con una instancia mayor en el caso que dicho incidente sobrepase el alcance del ERISD - ONPE.
- Debe facilitar la comunicación entre los diferentes Sub Gerencias que conforman el ERISD - ONPE.

Gestor de Incidentes de seguridad digital

- Un recurso en ONPE por el Sistema Electoral.
- Es el responsable de efectuar el informe de los incidentes de seguridad digital, analizar la implicancia legal del incidente en conjunto con el área funcional de jurídica/legal, coordinar las pruebas forenses, así como la mitigación, recuperación y apoyo a la gestión de la crisis ocasionada por el incidente.

Gestor de vulnerabilidades

- Un recurso en ONPE por el Sistema Electoral.
- Es el encargado del descubrimiento, análisis y manejo de vulnerabilidades de seguridad digital, nuevas o reportadas en los sistemas de información. Además, incluye servicios relacionados con la detección y respuesta a vulnerabilidades conocidas para evitar que sean explotadas.

Gestor de conocimiento situacional

- Un recurso en ONPE por el Sistema Electoral.
- Debe identificar, procesar, comprender y comunicar los elementos críticos del incidente, dentro y alrededor del área de los servicios afectados en su entidad.
- Es el responsable de realizar el comunicado en conjunto con el área funcional de comunicaciones/imagen institucional para los usuarios afectados.

Gestor de transferencia de conocimientos

- Un recurso en ONPE por el Sistema Electoral.
- Es el encargado de recopilar datos relevantes, realizar análisis detallados e identificar amenazas, tendencias y riesgos, así como crear las mejores prácticas operativas para ayudar a detectar, prevenir y responder a incidentes de seguridad digital.
- Es el encargado de difundir lecciones aprendidas de incidentes ocurridos, programar ejercicios de mitigación, así como establecer nuevas técnicas y políticas de mitigación en base a lecciones aprendidas.

Figura 3: Integrantes del ERISD-ONPE

Así mismo, si el alcance del incidente sobrepasa la capacidad de respuesta del ERISD-ONPE, el integrante que desempeña el rol Gestor de Incidentes de seguridad digital debe elevar dicho incidente a una instancia mayor como PCM - Centro Nacional de Seguridad Digital.

Funciones del ERISD-ONPE

El equipo de respuesta ante incidentes de seguridad digital – ERISD-ONPE, estará conformado por miembros de las Sub Gerencias que están dentro de la Gerencia Informática y Tecnología Electoral, en donde según la Resolución de Gerencia General N.º 000073-2021-GG/ONPE, articulo 2, se establece sus funciones, en el ámbito de su competencia:

a. Alinear sus acciones a las Políticas de Seguridad de la Información, Plan de recuperación de servicios de tecnologías de la información (Plan de Recuperación de Desastres) de la entidad.
b. Formular las estrategias, objetivos, planes, protocolos procedimientos y reglas para la gestión de incidentes de seguridad digital a nivel institucional y sectorial.
c. Monitorear y gestionar eventos de seguridad digital a nivel institucional.
d. Gestionar incidentes de seguridad digital a nivel institucional.
e. Comunicar al Centro Nacional de Seguridad Digital la existencia de incidentes de seguridad digital.
f. Mantener un registro de los incidentes de seguridad digital.
g. Conducir un análisis forense digital post-incidente, cuando sea necesario o cuando sea requerido, para identificar el origen del incidente.
h. Realizar periódicamente análisis de vulnerabilidades y pruebas de penetración a aplicaciones y servicios digitales de la entidad.
i. Mantener la operación, monitorización y actualización de dispositivos de seguridad interna y perimetral.
j. Colaborar con el Centro Nacional de Seguridad Digital la atención de un incidente de seguridad digital que afecte la seguridad nacional.
k. Realizar la coordinación con la Gerencia de Potencial Humano sobre el fortalecimiento de capacidades y competencias en seguridad digital a nivel institucional.
l. Difundir alertas tempranas, avisos e información sobre riesgos e incidentes de seguridad digital en la entidad y red de confianza.
m. Otras funciones en materia de seguridad digital que le asigne la Gerencia de Informática y Tecnología Electoral.

Por otra parte, se añade funciones pertinentes al ERISD-ONPE, como buena práctica para establecer puntos de mejora continua:

- Utilizar como mínimo herramientas de monitoreo e Inteligencia de amenazas dentro del proceso de Gestión de incidentes de Seguridad Digital.
- Contar como mínimo con personal especializado en inteligencia de amenazas cibernéticas y Gestión de Incidentes de seguridad digital, así como personal especializado de Análisis de Vulnerabilidades.
- Gestionar los incidentes de forma preventiva para analizar y tomar decisiones de forma coordinada y poder anticiparnosal impacto que pueda generar el incidente; con la finalidad de proteger los servicios y la infraestructura crítica que soporta al proceso electoral.
- Formular estrategias y procedimientos de mitigación ante incidentes de Seguridad Digital.
- Registrar y documentar la gestión de incidentes de Seguridad Digital.
- Interactuar con los encargados de análisis de vulnerabilidades, gestión de riesgos y hackeo ético.
- Gestionar todo el ciclo de vida de los incidentes de Seguridad Digital en relación con los Procesos Electorales.
- Realizar y ejecutar una mejorara continua, al proceso de clasificación de incidentes.
- Brindar respuesta oportuna a incidentes mediante una preparación, identificación contención, erradicación, recuperación y lecciones aprendidas.
- Definir estrategias para responder oportunamente ante intrusiones y/o amenazas
- Catalogar y definir los incidentes según su afectación tomando en cuenta los activos de información.
- Analizar y determinar el nivel de escalamiento según su criticidad para la institución.
- Establecer procedimientos de escalamiento ante incidentes de seguridad digital, estableciendo los contactos necesarios con los proveedores de servicios involucrados en el Proceso Electoral.
- Definir canales de comunicaciones y las entidades a quienes se derivan dichos incidentes de Seguridad Digital.
- Deberá realizar ejercicios de Seguridad Digital de manera periódica en cumplimiento al cronograma acordado.
- Utilizar una herramienta centralizada pararegistrar y gestionar los incidentes.

En coordinación con los integrantes del ERISD-ONPE se estableció que el alcance de la gestión de incidentes es desde la detección hasta la mitigación. En caso algún integrante del Sistema Electoral requiera denunciar el incidente, el ERISD-ONPE facilitará todas las evidencias que tenga a su alcance. En el siguiente diagrama se muestra el proceso para la gestión de los incidentes que se detecten en la etapa de monitoreo:

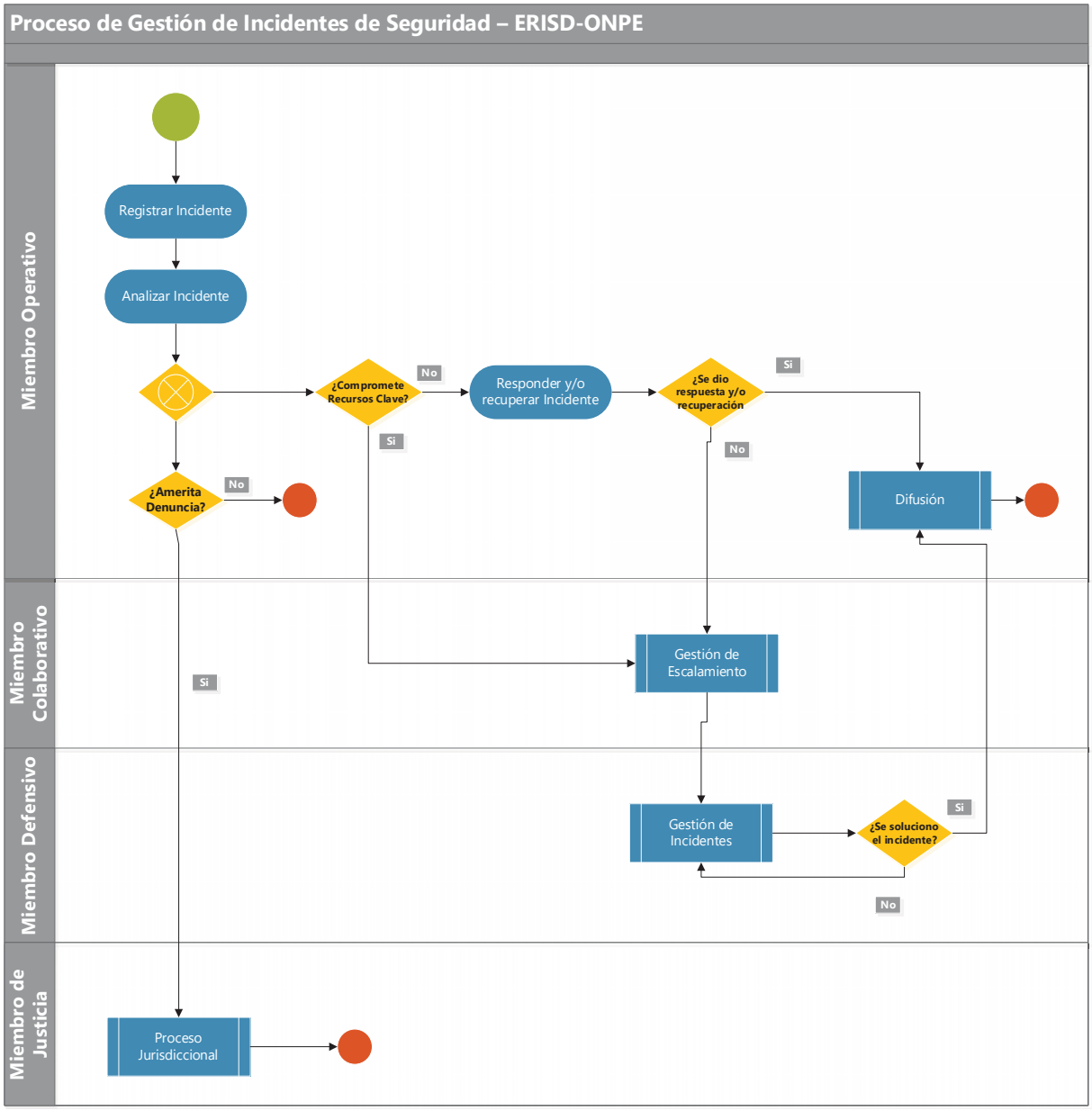


Figura 4: Gestión de incidentes de seguridad digital

Leyenda

Responsable	Unidades / Institución / Personal
Miembro Operativo	Especialista Técnico de las Sub-Gerencia
Miembro Colaborativo	Especialistas de las Sub-Gerencia
Miembro Defensivo	PCM - Consejo Nacional de Seguridad Digital ERISD -ONPE
Miembro de Justicia	Área Legal de ONPE

Todo incidente de seguridad digital de no poder contenerse y/o mitigar debe reportarse inmediatamente al Centro Nacional de Seguridad Digital correo: incidentes@cnsd.gob.pe y/o la plataforma https://facilita.gob.pe/t/1025

El Equipos de respuesta ante Incidentes de Seguridad Digital de la Oficina Nacional de Procesos Electorales deberá revisar periódicamente las alertas emitidas por el Centro Nacional de Seguridad Digital:

https://www.gob.pe/institucion/pcm/colecciones/791-alerta-integrada-de-seguridad-digital-del-cnsd

V. JUSTIFICACIÓN

5.1 Antecedentes

- El artículo 31 del Decreto Legislativo N.º 1412, que aprueba la Ley de Gobierno Digital, señala que el Marco de Seguridad Digital del Estado Peruano se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la confidencialidad, integridad, disponibilidad de la información en el entorno digital administrado por las entidades de la Administración Pública

- Mediante Decreto Supremo N.º 050-2018-PCM, publicado el 14 de mayo de 2018, se estableció la definición de Seguridad Digital de ámbito nacional, en el cumplimiento con la Segunda Disposición Complementaria Final de la Ley N°30618, Ley que modifica el Decreto Legislativo N°1441.

- Resolución de Gerencia General N.º 000073-2021-GG/ONPE, que constituye el “Equipo de Respuestas ante Incidentes de Seguridad Digital de la Oficina Nacional de Procesos Electorales ERISD de la ONPE” de naturaleza permanente, así como asignarle funciones en concordancia con lo previsto en el artículo 105 del Reglamento del Decreto Legislativo N.º 1412, aprobado por Decreto Supremo N.º 029-2021-PCM, de acuerdo con los términos propuestos por la Gerencia de Informática y Tecnología Electoral.

- Según la Resolución Jefatural N.º 003733-2022-JN/ONPE, (19 OCT 2022), se aprueba, el Plan Operativo Electoral Segunda Elección Regional 2022 versión 00.

- Resolución Jefatural N.° 004287-2022-JC/ONPE (10NOV2022) se aprueba, el Plan Operativo Electoral Segunda Elección Regional 2022 versión 01.

5.2 Problemática

La Oficina Nacional de Procesos Electorales – ONPE, incrementa la cantidad de activos de información en época electoral expuestos a internet por lo que genera mayor exposición a los diversos tipos ataques informáticos.

5.3 Análisis y evaluación de riesgo

Como parte del plan de ciberseguridad es necesario realizar una gestión de riesgos en los activos de información de la ONPE con el objetivo de verificar si los controles actuales son suficientes o es necesario aplicar controles para cerrar las brechas de ciberseguridad que mitiguen los riesgos identificados.

Los riesgos identificados y su nivel de riesgo se señalan en el siguiente cuadro:

	MATRIZ DE RIESGOS	Código	FM09-GPP/GC
		Versión	08
		Fecha de aprobación	27/10/2021
		Página	1 de 2

Fecha de Actualización: 07/11/2022 Nombre del proceso electoral: Segunda Elección Regional 2022 v00

IDENTIFICACIÓN DEL RIESGO Y OPORTUNIDADES Para ser llenado por el responsable del sistema de gestión de cada órgano y revisado por el responsable del proceso															ANÁLISIS Y EVALUACION DE RIESGOS Para ser llenado por el responsable del sistema de gestión de cada órgano y revisado por el responsable del proceso								
1. N°	2. FECHA DE IDENTIFICACIÓN	3. PROCESO NIVEL 1	4. OBJETIVO DE PROCESO	5. ACTIVIDAD	6. ACTIVO DE LA INFORMACIÓN EN CASO DE RIESGO DE SGSI	7. TIPO DE RIESGO	8. DESCRIPCIÓN DEL RIESGOS	9. CLASIFICACIÓN DEL RIESGO	10. PROPIETARIO DE RIESGO	11. SISTEMA DE GESTIÓN AFECTADO		12. NIVELES DE LOS PRINCIPIOS DE SGSI			13. CAUSAS	14. EFECTOS / CONSECUENCIAS	15. CONTROLES EXISTENTES	16. PROBABILIDAD (Po)		17. IMPACTO (I)		18. NIVEL RIESGO	
										SGC (Sistema de gestión de calidad)	SGSI (Sistema de gestión de seguridad de la información (Si afecta considerar el llenado desde el campo 11 al 13)	Confidencialidad	Integridad	Disponibilidad				VALOR	NIVEL	VALOR	NIVEL	VALOR	NIVEL
R1	07/11/2022	Tecnología de la Información	Brindar soporte a la institución en temas relacionados a las tecnologías de la institución.	Seguridad de la Información	Servicio Tecnológico	Negativo	Los Servicios Informáticos Electorales (páginas web y Apis) en la SER 2022 podrían ser vulnerados.	Tecnológico	GITE	X	X	1	1	2	Existen diferentes tipos de amenazas (programa maligno, malware, spam, ataque de DDoS, etc.) que atentan contra la información digital.	Pérdida de la integridad, confidencialidad y disponibilidad de la información.	1. Protección Perimetral (Firewall, IPS, Filtro WEB – AntiDDoS – Sandbox). 2. Protección Endpoint (Filtro de navegación - Antimalware – Prevención de Amenazas - MDM). 3. Protección Cloud (CDN –WAF - CASB). 4. Protección de Red (ISE - ACL)	3	Media	4	Alto	12	BAJO
R2	07/11/2022	Tecnología de la Información	Brindar soporte a la institución en temas relacionados a las tecnologías de la institución.	Seguridad de la Información	Servicio Tecnológico	Negativo	Incidentes complejos (ataques de DDoS, phishing, ransomware, malware, ataques de fuerza fruta) de ciberseguridad podrían presentarse en las SER 2022.	Tecnológico	GITE	X	X	1	1	2	Falta de capacidades tecnológicas.	Pérdida de la integridad, confidencialidad y disponibilidad de la información.	1. Servicio de análisis de Vulnerabilidades. 2. Conformación de un equipo de respuesta a incidentes (ERISD-ONPE). 3. Servicio de Ethical Hacking.	3	Baja	4	Medio	12	BAJO

NIVELES DE RIESGO INHERENTE Y MAPA DE CALOR

			IMPACTO NEGATIVO			
			BAJO	MEDIO	ALTO	MUY ALTO
			3	4	5	6
PROBABILIDAD	MUY ALTA	6	(18) MODERADO	(24) ALTO	(30) MUY ALTO	(36) MUY ALTO
	ALTA	5	(15) MODERADO	(20) MODERADO	(25) ALTO	(30) MUY ALTO
	MEDIA	4	(12) BAJO	(16) MODERADO	(20) MODERADO	(24) ALTO
	BAJA	3	(9) BAJO	(12) BAJO	(15) MODERADO	(18) MODERADO
			BAJO	MEDIO	ALTO	MUY ALTO
			3	4	5	6
			IMPACTO POSITIVO			

Riesgo Bajo	Riesgo Moderado	Riesgo Alto	Riesgo Muy Alto
9 – 12	15 - 20	24 – 25	30 – 36

VI. OBJETIVOS METAS E INDICADORES DEL PLAN

N°	DESCRIPCIÓN
A.	**Objetivo General:** Asegurar que los mecanismos de seguridad (tecnologías en Ciberseguridad) establecidos por ONPE, operen de forma adecuada para mantener la información integra, disponible, confidencial. **Objetivo Especifico:** Evitar incidentes a los activos informáticos que dan soporte a ONPE durante época electoral. **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

El porcentaje señalado en la meta es el valor deseado. Sin embargo, se establece niveles o escalas de evaluación que oriente las acciones estratégicas correctivas en caso no se alcance dicha meta, por el contrario, las oportunidades de mejora en caso de que la meta sea superada a fin de tender al 100%.

Mínimo Aceptable	Aceptable	Deseado	Satisfactorio	Sobresaliente
60% - 69.9%	70% - 99.9%	80%	80.1% - 89.9%	90% - 100%

VII. ESTRATEGIAS

La estrategia del Plan de Ciberseguridad está alineada al marco de Ciberseguridad NIST, esta estrategia debe ser aplicada de forma continua.

Además, establece la conformación de un “Equipo de Respuestas ante Incidentes de Seguridad Digital de la Oficina Nacional de Procesos Electorales – ERISD de la ONPE”, integrado con PCM- SEGDI- Centro Nacional de Seguridad Digital. El ERISD-ONPE debe operar alineado al marco del FISRT el cual establece los procesos y procedimientos de operación descritos en el presente Plan de Ciberseguridad.

VIII. ACTIVIDADES OPERATIVAS Y/O ACCIONES DEL PLAN

A continuación, se presenta en el formato FM09-GPP/PLAN, con la actividad operativa y tareas programadas para dicho plan:

	FORMATO	Código:	FM09-GPP/PLAN
	FORMULACIÓN/REPROGRAMACIÓN DE PLANES ESPECIALIZADOS Y DE ACCIÓN	Versión:	02
		Fecha de aprobación:	07/06/2019
		Página:	1 de 1

1. NOMBRE DEL PLAN - AÑO: PLAN DE CIBERSEGURIDAD PARA PROCESO ELECTORAL DE LA SER 2022 V00

2. ORGANO RESPONSABLE: GITE

15. Cód.	4.Actividad Operativa / Tarea / Acción	5.Unidad Orgánica responsable	6. Unidad de Medida	7.Sustento	8. Programación														
					Fecha		Meta Anual	Metas Físicas Mensuales											
					Inicio	Fin		Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
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																		
3.2.4.4	Gestionar servicios relacionados a Ciberseguridad y monitorear las herramientas de Ciberseguridad.	SGIST	Reporte	Reporte	01/11/2022	30/11/2022	2											1	1
3.2.4.5	Coordinar reuniones semanales con los integrantes del CSIRT Electoral.	SGIST	Reporte	Reporte	01/11/2022	31/12/2022	2											1	1

IX. PRESUPUESTO REQUERIDO

El presupuesto del Plan será el asignado para la ejecución de actividades en el marco del presupuesto institucional previsto para la ejecución del Plan Operativo Electoral, en la meta 59 de la GITE.

N° ITEM	Detalle del presupuesto requerido	Periodo	Cantidad	Monto
1	Servicio de Locador de servicios - Especialista de Ciberseguridad	Noviembre Diciembre 2022	1 persona	13,000.00
				Total: S/. 13,000.00

X. MONITOREO Y EVALUACIÓN

- El monitoreo del presente plan estará a cargo del Especialista en Ciberseguridad de la GITE o del personal de que la SGIST designe, y se llevará a cabo desde su aprobación. Así como, se realizará la evaluación del plan al término de la ejecución del mismo, en el formato FM11-GPP/PLAN.

XI. ANEXOS

a) Anexo “A” Procedimientos Operativos para reducir riesgos en contra de lainformación almacenada en las plataformas informáticas – POSI.
b) Anexo “B” Directorio Telefónico.
c) Anexo “C” Información sobre las sedes.
d) Anexo “D” Plan de Comunicaciones
e) Anexo “E” Agenda de Contactos
f) Anexo “F” Niveles de Probabilidad e Impacto

ANEXO A
PROCEDIMIENTOS OPERATIVOS PARA REDUCIR LOS RIESGOS EN CONTRA DE LA INFORMACIÓN ALMACENADA EN PLATAFORMAS INFORMÁTICAS

FUGA DE INFORMACIÓN DIGITAL

1. Sensibilizar al personal respecto a las buenas prácticas de seguridad digital.
2. Mantener actualizado el antivirus en todas las computadoras de la institución.
3. Mantener actualizado los softwares instalados en las computadoras de la institución.
4. Bloquear acceso de conexión de USB a las computadoras de la Red Electoral.
5. Restringir el acceso de conexión de dispositivos USB a las computadoras de la Red Administrativa.
6. No enviar por WhatsApp, correo electrónico, redes sociales u otros medios, fotografías, audios, videos, y cualquier otro tipo de archivos clasificados como información pública confidencial, reservada, secreta.
7. Bloqueo automático de las pantallas de las computadoras de la institución.
8. Restringir el acceso a correos electrónicos no institucionales desde computadoras de la institución.
9. Restringir el acceso a redes sociales, sistemas de mensajería instantánea, sistema de almacenamiento en la nube y cuentas de correo no institucional.
10. Restringir la copia de archivos en medios removibles de almacenamiento, USB, unidades ópticas de grabación en los equipos de cómputo de la entidad, la autorización debe ser gestionada por la GITE.
11. Implementar herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales, asimismo, controlar el acceso a la información contenida en portales de almacenamiento en el internet para prevenir la fuga de información.
12. Eliminar los correos desconocidos sin leerlos ni mucho menos accediendo a enlaces de páginas web que pueda contener en su mensaje.
13. Seleccionar contraseñas complejas (combinación de letras, números y caracteres especiales) en las cuentas de acceso a los sistemas de información. No compartirlas.
14. No extraer información de los equipos en dispositivos externos.
15. No hacer mal uso de los sistemas de información.
16. Los usuarios deben usar los equipos y accesorios que le han sido asignado únicamente para los fines que se le autorice.
17. Los usuarios de los sistemas de información e informáticos deben cerrar las aplicaciones y servicios de red cuando ya no les necesite.
18. Reportar el incidente de fuga de información digital al Centro de Atención de Usuarios de la GITE.
19. Todo incumplimiento de las disposiciones de seguridad de la información digital dará lugar a la investigación pertinente para determinar las causas y los correctivos que correspondan.
20. Apoyarse en el Equipo de Respuesta a Incidentes de Seguridad Digital – PECERT para resolver el incidente de fuga de información digital en caso sea necesario.
21. Solicitar apoyo al COCIB, si la situación lo amerita.
22. Denunciar el incidente de fuga de información digital a la DIVINDAT y la Fiscalía de la Nación.

INTERRUPCIÓN DE LOS SERVICIOS INFORMÁTICOS

1. Elaborar el plan de contingencias de Tecnologías de Información.
2. Implementar servicios informáticos de respaldo en el local alterno establecido.
3. Realizar el mantenimiento de los equipos informáticos de la institución.
4. Ejecutar copias de respaldo de la información en medios de almacenamiento masivo (cintas magnéticas).
5. Ejecutar escenarios de pruebas de contingencia de Tecnologías de Información.
6. Evaluar la ejecución de las pruebas de contingencias de Tecnologías de Información.

ANEXO B
DIRECTORIO TELEFÓNICO (*)

INSTITUCIÓN	NUMERO DE CONTACTO
DEFENSA CIVIL	110 / 225 – 9898
BOMBEROS	116
CENTRAL POLICIAL	105
POLICÍA DE TRÁNSITO	116
CENTRAL SAMU	399 – 3710
CENTRAL ONPE	417 – 0630
SEGURIDAD ONPE	980 212863 / 417 0630 (8782 – 8785)
LUZ DEL SUR	271 – 9090
ENEL	561 – 2001
SEDAPAL	317 – 8000
RADIO PATRULLA	977 144 373
CRUZ ROJA PERUANA	266 – 0481
TRANSITO PNP	324 – 8381
UDEX	431 – 3040
MENSAJES EN ZONAS DE EMERGENCIA	119
EMERGENCIAS MÉDICAS	112
CRUZ ROJA	115
DENUNCIA CONTRA VIOLENCIA FAMILIAR	100

(*) El directorio telefónico debe elaborarse en consideración a la ubicación de cada sede a nivel nacional.

ANEXO C
INFORMACIÓN SOBRE LAS SEDES DE LA ONPE (*)
SEDE CENTRAL

A. Ubicación Geográfica: (Av., Jr., Calle, N.º, Distrito, Provincia, Departamento). La sede central de la ONPE está ubicada en el Jirón Washington N° 1894 – Cercado de Lima.
Sus límites son: (Av., Jr., Calle)
- ✓ Por el Este: Jirón Washington.
- ✓ Por el Oeste: Avenida Guzmán Blanco.
- ✓ Por el Norte: Jirón Chincha.
- ✓ Por el Sur: Jirón Yauyos.

B. Nivel de Seguridad que se requiere: Alto, debido al personal, material y equipos electorales que se encuentran en su interior y que serán empleados en el presente proceso electoral.

C. Jurisdicción: A veintinueve (29) Centros de Cómputo organizados en veintisiete (27) Oficinas Descentralizadas de Procesos Electorales (ODPE) ubicadas a nivel nacional; tres (03) Centros de Cómputo de Contingencia – ORC (Arequipa, Chiclayo y Cusco), en la Sede Talara un (01) centro de cómputo de contingencia; centros de datos electorales y ambientes de apoyo al proceso Electoral en las sede central de la ONPE y en la sede Condevilla y ambientes para el taller de evaluación.

D. Información relevante:

(1) Centros de atención médica, como hospitales, clínicas, postas, otros.

LOCALIDAD	NOMBRE DEL CENTRO DE ATENCIÓN MÉDICA	DIRECCIÓN
Cercado-Lima	Policlínico Chincha	Jr. Chincha 226
Cercado-Lima	Clínica Internacional	Av. Garcilaso de la Vega 1420
Jesús María	Hospital Rebagliati	Av. Rebagliati 490
Cercado de Lima	Hospital Loayza	Av. Alfonso Ugarte 848
La Victoria	Hospital Almenara	Av. Miguel Grau 800

(2) Cuartel del cuerpo general de bomberos voluntarios del Perú:

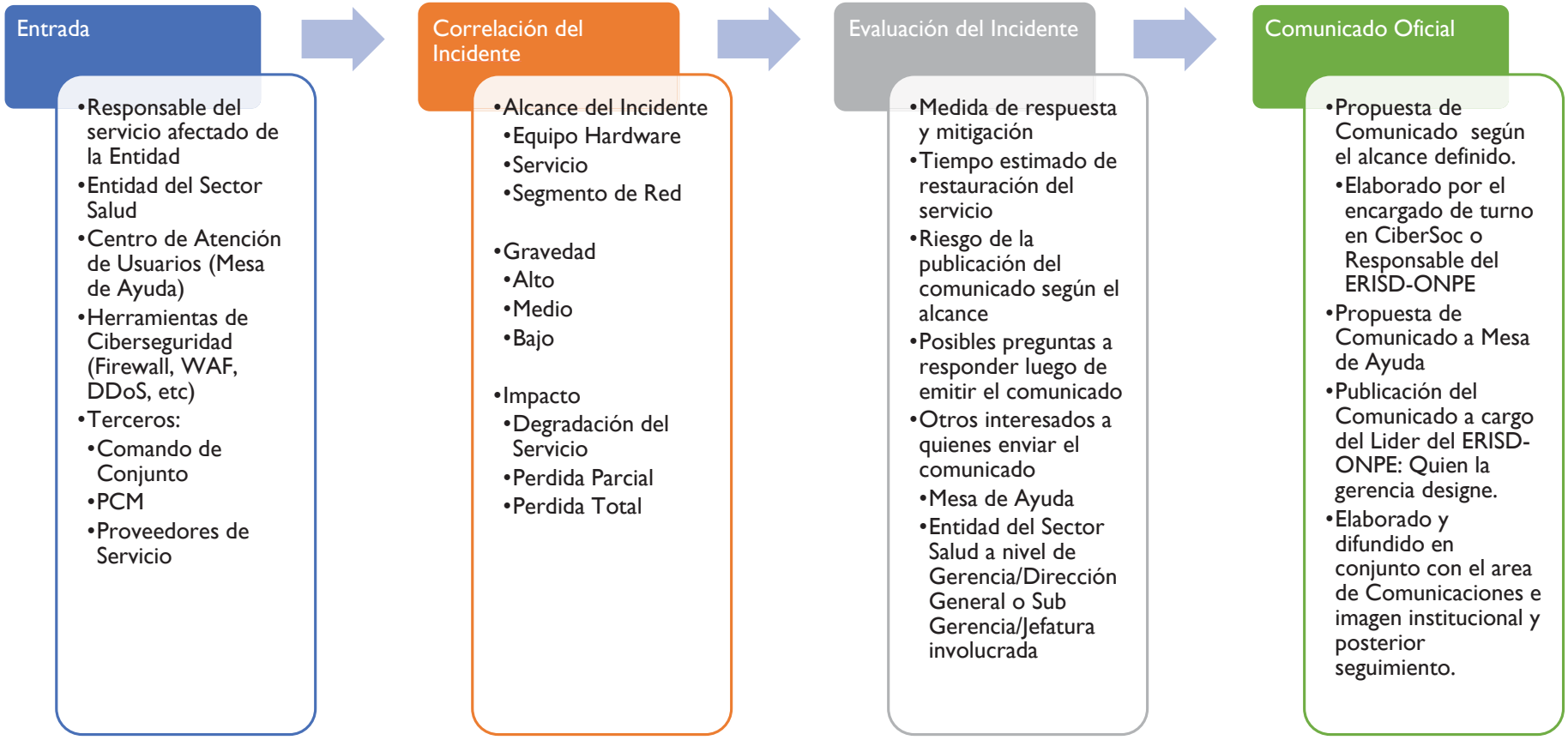
LOCALIDAD	NOMBRE DE LA COMANDANCIA	DIRECCIÓN
Cercado-Lima	Salvadora Lima	Jr. De la Unión 1001
Cercado-Lima	Cía. Bomberos France 3	Jr. Moquegua 240
Cercado de Lima	Cía. Bomberos Roma 2	Jr. Junín 568

(3) Dependencias Militares y Policiales

LOCALIDAD	NOMBRE DE LA DEPENDENCIA	DIRECCIÓN
Cercado-Lima	Comando Conjunto FFAA	Jr. Nicolás Corpancho N° 289-Santa Beatriz Alt. Cdra. 2 Av. Arequipa. – LIMA
Jesús María	Comandancia General de la Fuerza Aérea	Av. La Peruanidad S/N
Cercado de Lima	Comisaria Petit Thouars	Av. Petit Thouars 455

- No existe antecedentes recientes de enfrentamientos armados con terroristas.
- Las denuncias policiales y/o actividades delictivas que más destacan son: Hurto, arrebato, agresión, violencia familiar.
- Se ha previsto comunicación con las Autoridades Militares a efectos de contar con su apoyo cada vez que la situación lo requiera.
- Se ha previsto comunicación con las Autoridades Policiales a efectos de contar con su apoyo cada vez que la situación lo requiera.

ANEXO D
PLAN DE COMUNICACIONES



ANEXO E
PERSONAL DE LAS UNIDADES QUE SON PARTE DEL SISTEMA ELECTORAL
Matriz de contactos de ONPE

Según la resolución de Gerencia General N.º 000073-2021-GG/ONPE en el artículo primero se conforma el Equipos de Respuesta ante Incidentes de Seguridad Digital (ERISD-ONPE) a nivel de Unidad Orgánica.

Unidad Orgánica	Función
Gerente de la Gerencia de Informática y Tecnología Electoral (GITE)	Miembro y lo Preside
Sub Gerencia de Gobierno Digital e Innovación (SGGDI)	Miembro
Sub Gerente de Operaciones Informáticas (SGOI)	Miembro
Sub Gerencia de Sistemas de Información (SGSI)	Miembro
Sub Gerente de Infraestructura y Seguridad Tecnológica (SGIST)	Miembro y Coordinador del equipo de respuestas
Coordinador de Mesa de Ayuda	Miembro
Oficial de Seguridad y Confianza Digital	Miembro

Contactos responsables para operación y/o escalamientos técnicos

CONTACTOS ERISD-ONPE				
Función ERISD	**Nivel de Escalamiento**	**Unidad Orgánica**	**Nombre y Apellidos**	**Correo**
Coordinador ERISD	Nivel 1	SGIST	Carlos Arroyo Marticorena	carroyom@onpe.gob.pe
Gestor de Redes y Comunicaciones	Nivel 1	SGIST	Miguel Polo Palacios	mpolo@onpe.gob.pe
Gestor de Infraestructura Digital	Nivel 1	SGIST	Manuel Marin Flores	mmarin@onpe.gob.pe
Gestor de Infraestructura Digital	Nivel 1	SGIST	Javier Huaman Martinez	jhuamanm@onpe.gob.pe
Coordinador ERISD	Nivel 2	SGOI	Eddy Lucila Torre Ostos	etorre@onpe.gob.pe
Coordinador ERISD	Nivel 2	SGGDI	Jackeline Chacon Terrones	jchacon@onpe.gob.pe
Coordinador ERISD	Nivel 2	SGSI	Napoleon David Posada Pajuelo	nposada@onpe.gob.pe
Líder Técnico	Nivel 3	SGIST	José E. Samame Blas	jsmame@onpe.gob.pe
Líder	Nivel 4	GITE	Roberto Carlos Montenegro Vega	rmontenegrov@onpe.gob.pe

ANEXO E
NIVEL DE LOS PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

NIVEL	Concepto	Valor	Descripción de los valores de los principios de SGSI
Confidencialidad	Propiedad que hace que información no se haga accesible o revelada a individuos, entidades o procesos no autorizados	**1**	No se ve afectada la confidencialidad de la información.
		2	Significa una pérdida de la confidencialidad de la información del proceso o proyecto . La información puede ser accedida por personas no autorizadas.
Integridad	Propiedad que hace que la información sea precisa y completa.	**1**	No se pierde la integridad de la información.
		2	Se pierde la integridad de la información. Por ejemplo: la información se encuentra adulterada de manera remota o manual.
Disponibilidad	Propiedad que hace que la información sea accesible y útil a pedido, por un ente autorizado.	**1**	No se pierde la disponibilidad de la información.
		2	Se pierde la disponibilidad de la información. Como, por ejemplo: información no ubicada en su lugar.

NIVEL O PARÁMETROS DE PROBABILIDAD

NIVEL DE PROBABILIDAD	VALOR	DESCRIPCIÓN DE LA PROBABILIDAD	CRITERIO (*)
Baja	3	Existen condiciones escasamente propicias para que ocurra el evento. Riesgo cuya probabilidad de ocurrencia es baja.	No se ha producido situaciones similares en un proceso electoral / proyecto o en el año de corresponder
Media	4	Existen condiciones medianamente propicias para que ocurra el riesgo. Riesgo cuya probabilidad de ocurrencia es media.	Se ha producido al menos en 1 proceso electoral/ proyecto o 1 vez en el año de corresponder.
Alta	5	Existen condiciones altamente propicias para que ocurra el riesgo.Riesgo cuya probabilidad de ocurrencia es alta.	Se ha producido al menos en 2 procesos electorales/proyecto o 2 veces en el año de corresponder
Muy Alta	6	Existen condiciones extremadamente propicias para que ocurra el riesgo.Riesgo cuya probabilidad de ocurrencia es muy alta.	Se ha producido en 3 o más de 3 procesos electorales/ proyecto o 3 veces en el año de corresponder.

NIVEL O PARAMETROS DEL IMPACTO

NIVEL DEL IMPACTO + o -	VALOR	DESCRIPCIÓN DEL IMPACTO NEGATIVO	DESCRIPCION DEL IMPACTO POSITIVO
Bajo	3	El riesgo causaría un bajo o nulo efecto o impacto en la ONPE, que no paraliza la continuidad de las operaciones.	Si el evento llegara a presentarse, no representa un impacto positivo para la organización.
Medio	4	El riesgo causaría un daño importante o significativo, pero que es superable o contrarrestable con cierta dificultad y que no afecta a los objetivos estratégicos.	Si el evento llegara a presentarse, tendría un impacto positivo de menor prioridad ya que el efecto de la oportunidad es sobre algunas actividades críticas de la organización.
Alto	5	El riesgo cuya materialización causaría gravemente un daño importante o significativo de la imagen. Además, se requeriría una cantidad de tiempo importante en investigar y corregir los daños.	Si el evento llegara a presentarse, tendría un impacto positivo en el desempeño de los procesos de soporte de la organización.
Muy Alto	6	El riesgo cuya materialización dañaría significativamente a la imagen o logro de los objetivos de la entidad. Además, se requeriría una cantidad importante de tiempo de la alta dirección en corregir los daños.	Si el evento llegara a presentarse, tendría un impacto positivo en el desempeño de los procesos principales de la organización