"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la lucha contra la corrupción y la impunidad"

Lima, 16 de Diciembre del 2019

RESOLUCION JEFATURAL N° 000274-2019-JN/ONPE

VISTOS: los Memorando N° 000697-2019-OSDN/ONPE, N° 000713-2019-OSDN/ONPE e Informe N° 000031-2019-OSDN/ONPE de la Oficina de Seguridad y Defensa Nacional; el Memorando N° 003870-2019-GPP/ONPE, de la Gerencia de Planeamiento y Presupuesto; así como, el Informe N° 000480-2019-GAJ/ONPE, de la Gerencia de Asesoría Jurídica; y,

CONSIDERANDO:

Mediante Decreto Supremo N° 165-2019-PCM, publicado en la edición extraordinaria del diario oficial El Peruano, del 30 de setiembre de 2019, el Presidente de la República convocó a elecciones para un nuevo Congreso, para el día domingo 26 de enero de 2020, para que complete el periodo constitucional del Congreso disuelto;

De conformidad con el literal f) del artículo 5 de la Ley N° 26487, Ley Orgánica de la Oficina Nacional de Procesos Electorales (ONPE), este organismo constitucional autónomo tiene como función, entre otras, dictar las instrucciones y disposiciones para el mantenimiento del orden y la protección de la libertad personal durante los comicios;

De acuerdo al artículo 40 de la Ley N° 26859, Ley Orgánica de Elecciones, la ONPE dicta las instrucciones y disposiciones necesarias para asegurar el mantenimiento del orden público y la libertad personal durante los comicios, las cuales son obligatorias y de estricto cumplimiento para la Policía Nacional y las Fuerzas Armadas;

Por otro lado, conforme al literal p) del artículo 11 del Texto Integrado del Reglamento de Organización y Funciones de la ONPE, aprobado por Resolución Jefatural N° 000246-2019-JN/ONPE, corresponde a la Jefatura Nacional aprobar las disposiciones necesarias que garanticen el mantenimiento del orden y la protección de la libertad personal durante los comicios;

En el marco legal antes anotado, la Oficina de Seguridad y Defensa Nacional, a través del Informe de vistos formula su propuesta del Plan de Seguridad para las "Elecciones Congresales Extraordinarias 2020" Versión 00, justificándolo en la necesidad de disponer de una herramienta de gestión que oriente acerca de las estrategias por seguir, para que las actividades previstas en el marco del citado proceso electoral, se desarrolle en condiciones adecuadas de seguridad, incluyendo medidas para proteger la confidencialidad, integridad y disponibilidad de la información de la Entidad;

Por su parte, la Gerencia de Planeamiento y Presupuesto mediante el Memorando de vistos, adjuntando el Informe N° 000855-2019-SGPL-GPP/ONPE de la Sub Gerencia de Planeamiento, brinda opinión técnica favorable al Plan de Seguridad propuesto por la Oficina de Seguridad y Defensa Nacional, concluyendo que se encuentra alineado al Plan Operativo Electoral ECE 2020, Versión 01; cumpliendo, además, con la estructura determinada en el Anexo 6.8 del Instructivo: IN 01-GPP/PLAN, Versión 03, Formulación, Reprogramación, Monitoreo y Evaluación de Planes Institucionales;

De conformidad con lo dispuesto en el literal f) del artículo 5 de la Ley N° 26487, Ley Orgánica de la Oficina Nacional de Procesos Electorales y el literal p) del artículo 11 del Texto Integrado de su Reglamento de Organización y Funciones, aprobado por Resolución Jefatural N° 000246-2019-JN/ONPE;

Con el visado de la Secretaría General, de la Oficina de Seguridad y Defensa Nacional, así como de las Gerencias de Asesoría Jurídica y de Planeamiento y Presupuesto;

SE RESUELVE:

Artículo Primero.- Aprobar el Plan de Seguridad para las "Elecciones Congresales Extraordinarias 2020", Versión 00, cuyo texto en anexo forma parte integrante de la presente Resolución Jefatural.

Artículo Segundo.- Encargar a la Oficina de Seguridad y Defensa Nacional, efectuar el seguimiento y ejecución del Plan de Seguridad, aprobado conforme al artículo que antecede.

Artículo Tercero.- Disponer que el cumplimiento del Plan de Seguridad para las "Elecciones Congresales Extraordinarias 2020", Versión 00, será responsabilidad de todos los órganos de la entidad.

Artículo Cuarto.- Disponer la publicación de la presente resolución y sus anexos en el portal institucional, www.onpe.gob.pe y en el portal de Transparencia de la ONPE, dentro del plazo de tres (3) días de su emisión.

Regístrese y comuníquese.

MANUEL FRANCISCO COX GANOZA
Jefe (i)
Oficina Nacional de Procesos Electorales

MCG/ght/mbb/acp

Firma Digital

Firmado digitalmente por IGLESIAS AREVALO Walter Mauro FAU 20291973851 soft
Motivo: Soy el autor del documento
Fecha: 12.12.2019 17:04:42 -05:00

ONPE
OFICINA NACIONAL DE PROCESOS ELECTORALES

PLAN DE SEGURIDAD

ELECCIONES CONGRESALES EXTRAORDINARIAS 2020

OFICINA DE SEGURIDAD Y DEFENSA NACIONAL

Diciembre, 2019

Versión 0.0

Firma Digital

Firmado digitalmente por ALIAGA GASTELUMENDI Hugo Armando FAU 20291973851 soft
Motivo: Doy V° B°
Fecha: 13.12.2019 09:23:44 -05:00

Firma Digital

Firmado digitalmente por PACHECO HERRERA Leslie Edilma FAU 20291973851 soft
Motivo: Doy V° B°
Fecha: 12.12.2019 18:58:15 -05:00

Firma Digital

Firmado digitalmente por VARGAS FIERRO Milagros Judith FAU 20291973851 soft
Motivo: Doy V° B°
Fecha: 12.12.2019 18:08:37 -05:00

Firma Digital

Firmado digitalmente por BIGGIO PASTOR Maria Del Pilar FAU 20291973851 soft
Motivo: Doy V° B°
Fecha: 12.12.2019 17:43:42 -05:00

Firma Digital

Firmado digitalmente por TWANAMA ALTAMIRANO Walter Paul FAU 20291973851 soft
Motivo: Doy V° B°
Fecha: 13.12.2019 09:11:58 -05:00

Firma Digital

Firmado digitalmente por TILLIT ROIG Maria Elena FAU 20291973851 soft
Motivo: Doy V° B°
Fecha: 12.12.2019 18:44:57 -05:00

Firma Digital

Firmado digitalmente por PUYO VALLADARES Roberto Rori FAU
oft
°
19 17:55:45 -05:00

ÍNDICE

ABREVIATURAS

Centro de Operaciones de Procesos Electorales ..... COPE
Comando Conjunto de las Fuerzas Armadas ..... CCFFAA
Comandante General de la Policía Nacional del Perú..... CGPNP
Comando Operacional de Ciberdefensa ..... COCIB
Cuerpo Voluntario de Bomberos del Perú ..... CVBP
Defensoría del Pueblo ..... DP
Dirección de Inteligencia de la PNP… ..... DIRIN
División de Investigaciones de Delitos de Alta Tecnología..... DIVINDAT
Dirección Nacional de Inteligencia ..... DINI
Gerencia de Comunicaciones y Relaciones Corporativas..... GCRC
Gerencia Corporativa de Potencial Humano ..... GCPH
Gerencia de Gestión de Calidad ..... GGC
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
Jefatura Nacional ..... JN
Jefe de Oficina Descentralizadas de Procesos Electorales..... JODPE
Jurado Electoral Especial ..... JEE
Jurado Nacional de Elecciones..... JNE
Ministerio Público..... MP
Oficina Descentralizada de Proceso Electorales ..... ODPE
Oficina Nacional de Procesos Electorales..... ONPE
Oficina Regional de Coordinación..... ORC
Oficina de Seguridad y Defensa Nacional..... OSDN
Policía Nacional del Perú..... PNP
Proyecto Especial de Infraestructura de Transporte Nacional..... PROVIAS NACIONAL
Registro Nacional de Identificación y Estado Civil..... RENIEC
Secretaría General ..... SG
Sub Comandancia General de la Policía Nacional del Perú..... SCGPNP
Subgerencia de Operaciones Electorales ..... SGOE
Unidad de Desactivación de Explosivos..... UDEX

I. INTRODUCCIÓN

El presente Plan de Seguridad ha sido elaborado con la finalidad de disponer de una herramienta de gestión que oriente acerca de las estrategias por seguir para que las actividades previstas en el marco de las Elecciones Congresales Extraordinarias 2020, que se realizarán el día domingo 26 de enero de 2020, se desarrollen en condiciones adecuadas de seguridad.

Siendo la información uno de los principales activos de la entidad, el Plan contempla además medidas para proteger su confidencialidad, integridad y disponibilidad.

En este contexto, se sugieren, acciones de carácter preventivo y otras que corresponden a momentos de actuación frente a peligros y riesgos que podrían presentarse.

El éxito en su ejecución dependerá de la organización, colaboración, participación, comunicación, coordinación y del compromiso de las instancias involucradas.

II. MARCO LEGAL

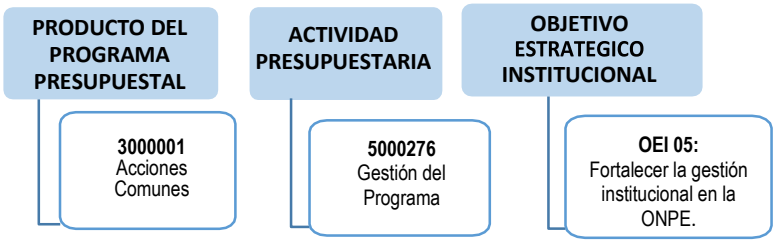
- Constitución Política del Perú.
- Ley N° 26859, Ley Orgánica de Elecciones y sus modificatorias.
- Ley N° 26487, Ley Orgánica de la Oficina Nacional de Procesos Electorales.
- Ley N° 26300, Ley de los Derechos de Participación y Control Ciudadanos.
- Ley N° 29973, Ley General de la Persona con Discapacidad.
- Ley N° 28983, Ley de igualdad de oportunidades entre mujeres y hombres.
- Ley N° 28094, Ley de Organizaciones Políticas y sus modificatorias.
- Ley N° 28863, Ley que modifica los artículos 7, 9 y 16 de la Ley N° 27933, Ley del Sistema Nacional de Seguridad Ciudadana.
- Ley N° 29478, Ley que establece facilidades para la emisión del voto de las personas con discapacidad.
- Ley N° 30999, Ley de Ciberdefensa.
- Decreto Legislativo N° 635, Código Penal.
- Decreto Supremo N° 165-2019-PCM, Decreto Supremo que disuelve el Congreso de la República y convoca a elecciones para un nuevo Congreso.
- Resolución Suprema N° 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 Ministerial N° 004-2016-PCM (08ENE2016) 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”.
- Resolución Jefatural N° 000093-2017-J/ONPE, que aprueba la Directiva Lineamientos de Seguridad de la Información, con Código DI04-GGC/GC.
- Resolución Jefatural N° 000094-2017-J/ONPE, que aprueba la Política y los Objetivos de Seguridad de la Información.
- Resolución Jefatural N° 000108-2019–JN/ONPE (29MAR2019), que aprueba el Plan Estratégico Institucional 2018-2022 de la ONPE.
- Resolución Jefatural N° 000246-2019–JN/ONPE (25NOV2019), que aprueba el Texto Integrado del Reglamento de Organización y Funciones de la Oficina Nacional de procesos Electorales que fue aprobado con Resolución Jefatural N° 063-2014-J/ONPE con las modificaciones contenidas en las Resoluciones Jefaturales Nros. 216-2014-J/ONPE, 0122-2015-J/ONPE, 000012-2017-J/ONPE y 000183-2019-JN/ONPE

- Resolución Jefatural N° 000256-2019–JN/ONPE (03DIC2019), que aprueba el "Plan Operativo Electoral Elecciones Congresales Extraordinarias 2020 Modificado Versión 01"- ECE2020.

III. MARCO ESTRATÉGICO

3.1 ALINEACIÓN DE OBJETIVOS

Los procesos, sus actividades operativas, tareas y acciones se formulan en función a los objetivos del Plan Operativo Electoral, alineados al objetivo estratégico del Plan Estratégico Institucional 2018-2022 (PEI 2018-2022).



3.2 GENERALIDADES DEL PROCESO ELECTORAL

Mediante Decreto Supremo N° 165-2019-PCM, el Presidente de la República convocó a Elecciones Congresales Extraordinarias para el día 26 de enero del 2020, con la finalidad de elegir un nuevo Congreso que complete el periodo constitucional del Congreso disuelto incluida la Comisión Permanente.

FICHA TÉCNICA DE LAS ECE 2020 - V04

(Al 6 de diciembre de 2019)

Item	Descripción	Elecciones Congresales Extraordinarias 2020					
1	Proceso						
2	Ámbito	Nacional y extranjero					
3	Periodicidad	Variable					
4	Fecha de elección	26 de enero de 2020					
5	ODPE a/	60					
6	Tipo de Tecnología b/	Nacional				Extranjero	TOTAL
		Voto Electrónico		CON	Total Nacional	CON	
		VEP	SEA				
7	Electores Hábiles c/	1 768 530	931 585	21 125 039	**23 825 154**	974 230	**24 799 384**
8	Mesas de Sufragio d/	5 359	2 866	73 252	**81 477**	3 374	**84 851**
9	Locales de Votación e/	266	219	4 693	**5 178**	231	**5 409**
10	Distritos b/	39	96	1 739	**1 874**	221	**1,874 distritos 221 ciudades**

Notas:

- Se considera instalación de mesas especiales
- Se considera, en promedio, 280 electores en CCPP (excepto Lima) y máximo 350 electores en VEP/SEA y 300 electores en CON.
- Existen 14 países en el extranjero con menos de 25 electores.

a/ De acuerdo con la resolución jefatural 206-2019-JN/ONPE (12OCT2019).

b/ Con base en las tecnologías usadas en el Referéndum Nacional 2018 y las EMC 2019.

c/ Resolución N° 0190-2019-JNE (16NOV2019)

d/ Producto del proceso de conformación de mesas de sufragio.

e/ Información histórica respecto del ámbito nacional e información proyectada respecto del ámbito extranjero

VEP: Voto Electrónico Presencial
SEA: Sistema de Escrutinio Automatizado
CON: Convencional

Fuente: Memorando Múltiple n.º 157-2019-GPP/ONPE (06DIC2019)

IV. JUSTIFICACIÓN

La elaboración del presente plan se justifica en el interés de fortalecer la cultura y conciencia de seguridad, y en la necesidad de:

1. Administrar la seguridad con medidas y acciones que demuestren organización, planificación, coordinación, participación, prevención, para atender situaciones de peligro o de riesgo que podrían afectar la seguridad del proceso electoral y que, además, involucren a los Organismos del Sistema Electoral (JNE, RENIEC, ONPE), así como, a las FFAA y PNP.

2. Proteger la información institucional, en cualquiera de las formas en que se maneje (impresa, escrita en papel, almacenada electrónicamente, transmitida por correo, por redes sociales u otros medios electrónicos, mostrada en videos, en fotos, así como expuesta oralmente o en conversaciones).

4.1 PROBLEMÁTICA

a. Posibles grupos de personas inescrupulosas pretendan impedir el normal desarrollo de las actividades previstas, en el marco de las Elecciones Congresales Extraordinarias 2020, que se realizarán el día domingo 26 de enero de 2020, atentando contra el personal, las instalaciones, los bienes y el material electoral.

b. Que como consecuencia de la coyuntura social y política, se presenten manifestaciones en contra de los organismos electorales, las que podrían descontrolarse terminando en disturbios, agresiones, toma de locales y otras expresiones de violencia.

c. Posible fuga de información institucional, especialmente aquella relacionada al proceso electoral, lo que ocasionaría desconfianza en la ciudadanía y desacreditación de la entidad.

4.2 RIESGOS QUE PODRÍAN AFECTAR EL PROCESO ELECTORAL

4.2.1 Riesgos en contra de las personas, de las instalaciones, de los bienes y del material electoral

(a) Intrusión

(b) Toma de local

(c) Robo

(d) Asalto

(e) Disturbios

(f) Conflictos sociales

(g) Atentados terroristas

(h) Accidentes de tránsito

(i) Agresiones físicas

(j) Extorsión

(k) Corrupción

(l) Infidencia

(m) Sabotaje

(n) Infiltración

(o) Espionaje

(p) Clima laboral no óptimo

(q) Interrupción del fluido eléctrico

(r) Inundación

(s) Emergencias por salud

(t) Sismo
(u) Incendio
(v) Tsunami
(w) Riesgos generados por condiciones climatológicas
(x) Fuga de información física

4.2.2 Riesgos en contra del material electoral durante su desplazamiento

(a) Emboscada

(b) Accidentes de tránsito

(c) Secuestro

4.2.3 Riesgos en contra de la información almacenada en las plataformas informáticas

(a) Fuga, modificación, retiro, destrucción, de información digital (por virus, extracción usando dispositivos externos, correo electrónico, redes sociales, etc.).

(b) Interrupción de servicios informáticos (página web, voto electrónico, etc.)

4.3. OTROS ASPECTOS PARA CONSIDERAR

4.3.1 Puntos vulnerables

Los puntos vulnerables para tomar en cuenta son:

a) Personas

- ✓ Servidores y personal contratado por los Organismos Electorales: de la Oficina Nacional de Procesos Electorales - ONPE, del Jurado Nacional de Elecciones - JNE, del Registro Nacional de Identificación y Estado Civil – RENIEC, en especial sus autoridades y responsables de los procesos críticos *logísticos e informáticos).

- ✓ Personal que da servicio de seguridad y vigilancia en las sedes de la ONPE, JNE, RENIEC.

- ✓ Personal de las Fuerzas Armadas – FFAA y de la Policía Nacional del Perú – PNP, involucrados en la seguridad de las actividades del Proceso Electoral.

4.3.2 Instalaciones, bienes e información

- ✓ Locales principales de la ONPE, del JNE y del RENIEC.
- ✓ Instalaciones de los organismos electorales que contienen personas, bienes, equipos e información sensible para el presente proceso electoral.
- ✓ Sedes en donde operan las Oficinas Descentralizadas de Procesos Electorales - ODPE, las Oficinas Regionales de Coordinación - ORC y los Jurados Electorales Especiales – OJEE.
- ✓ Locales donde se imprime el material electoral.
- ✓ Locales donde se prepara el material electoral para su distribución.
- ✓ Locales donde se almacenan equipos y material electoral.
- ✓ Equipos de cómputo que se emplearán para el voto electrónico.
- ✓ Locales de votación.

4.3.3 Transporte del material electoral

- ✓ Medio previsto para el transporte del personal, de los bienes y material electoral (terrestre, acuático, aéreo).
- ✓ Actividades relacionadas con la carga y descarga del material electoral.
- ✓ Actividades relacionadas con el desplazamiento de personal y material electoral:

  (-) Para impresión, preparación, capacitación y almacenamiento.

  (-) Durante el despliegue y repliegue desde Lima hacia las ODPE,

  oficinas distritales, centros de votación y viceversa.
- ✓ Rutas principales y alternas.

4.3.4 Infraestructura tecnológica electoral

- ✓ Red Electoral
- ✓ Software de cómputo de resultados y de voto electrónico.

V. OBJETIVO

Determinar estrategias para la protección del personal, de los bienes, de los materiales y de la información, involucrados en el presente proceso electoral, reduciendo consecuentemente los peligros, las vulnerabilidades y riesgos.

METAS E INDICADORES

Para el presente plan, se establece el siguiente indicador:

Nº	Indicador	Meta	Responsable
01	Número de capacitaciones otorgadas por la OSDN en materia de seguridad para el personal de ODPE y GIEE	03	OSDN
02	Porcentaje de sedes de los organismos electorales que cuentan con custodia policial, hasta un mes antes del día del sufragio	80%	OSDN
03	Porcentaje de atención oportuna de los Resguardos solicitados para el desplazamiento del material electoral	90%	OSDN
04	Número de coordinaciones con la DIVINDAD y COCIB para contar con apoyo técnico en materia de seguridad informática	03	GITE

VI. ESTRATEGIAS

El presente plan ha previsto atender la seguridad antes, durante y después del proceso electoral para ello cuenta con las siguientes estrategias:

- Acciones de coordinación externa, con las FFAA, PNP, JNE, RENIEC, MP, DP, PCM, DINI, DIRIN COCIB, DIVINDAT, entre otras entidades, para compartir información, brindar y/o recibir asesoramiento y apoyo que coadyuve al desarrollo del proceso electoral (antes, durante y después), según competencias.
- Acciones de coordinación interna, con las unidades orgánicas de la ONPE involucradas en el desarrollo del proceso electoral, con la finalidad de brindar el asesoramiento y determinar las actividades que requieren apoyo de seguridad.
- Acciones de coordinación con el Oficial de seguridad de la Información y con el Comité de Gestión de Seguridad de la Información, asuntos relacionados a la seguridad de la información de la entidad.
- Acciones de capacitación sobre las medidas de seguridad del proceso electoral (plan de seguridad, matriz y mapa de riesgos electorales, manejos de conflictos, gestión del riesgo de desastre).
- Determinación de responsabilidades de seguridad, a fin de administrar preventivamente la seguridad, contando con la participación e involucramiento de las unidades orgánicas, según competencias.
- Optimizar los niveles de comunicación, a fin de que toda actividad o situación especial que requiera el apoyo de seguridad**,** sea comunicada oportunamente a la OSDN, para la atención correspondiente.
- Elaboración de matriz y mapa de riesgos electorales.
- Elaboración de “Procedimientos Operativos de Seguridad”, para atender los riesgos previstos en el presente Plan (Anexo A).

- Supervisión de los servicios de seguridad y vigilancia, contratados por la entidad.
- Seguimiento a la atención de las necesidades de seguridad de las ECE 2020, especialmente aquellas relacionadas a la custodia de los locales y el resguardo de los equipos y material electoral.

6.1 Fase Previa

a. En esta fase, la ONPE, el Reniec y el JNE deben de efectuar el máximo de coordinaciones con la finalidad de establecer sus necesidades de seguridad.

b. El Reniec y el JNE deben de solicitar formal y oportunamente sus necesidades de seguridad (precisando actividades, fechas, horarios, lugares, entre otros), a fin de que la ONPE proceda a efectuar las actividades de planificación y coordinación para que el CCFFAA y la PNP proporcionen la atención correspondiente, según sus competencias.

c. El JNE, la PCM, DP, la DINI, el CCFFAA, la PNP, la ONPE entre otras instituciones compartirán información que coadyuve a la adopción de medidas en beneficio de la seguridad de las ECE-2020.

d. La ONPE, el JNE y el Reniec deben adoptar medidas para que la selección de personal que apoyará en este proceso electoral contemple filtros básicos que minimicen la posibilidad de que se presenten situaciones que podrían tener impacto negativo, tales como: infiltración, ingreso de personas que no tengan las competencias para el puesto, personas con antecedentes policiales, penales, con filiación a partidos políticos, entre otros.

e. La ONPE, el JNE y el Reniec deben realizar simulacros de evacuación por emergencia: incendio, sismo, tsunami, detección de artefactos explosivos, entre otros, a fin de preparar al personal y reducir posibles daños.

f. La ONPE, el JNE y el Reniec deben realizar capacitaciones en asuntos relacionados a la seguridad del proceso, Gestión de Riesgos de Desastres y ejecución de sus respectivos planes de seguridad, como parte de las medidas preventivas de seguridad.

g. Las Gerencias de la ONPE deben de identificar las actividades, los momentos y los lugares que requieren la ejecución de medidas de seguridad, procediendo a administrar las que son de su competencia, y las que requieren atención especial serán motivo de coordinación con la OSDN.

h. El Oficial de Seguridad de la Información y el Comité de Gestión de Seguridad de la información, con el apoyo de la GITE, SG, OSDN y otros órganos (según competencias), deben de elaborar, revisar, actualizar, aprobar, difundir, los documentos de seguridad de información que sean pertinentes (políticas, objetivos, lineamientos, plan, entre otros), para la aplicación respectiva.

i. La GITE debe determinar roles, funciones, responsabilidades, de operación y administración de los sistemas informáticos, incluido los teléfonos e impresoras.

j. La OSDN, debe determinar medidas para el ingreso de dispositivos móviles (teléfonos celulares, tabletas, laptop, cámaras fotográficas y de video, grabadores, entre otros).

k. La OSDN, GITE, GCRC (según competencias), deben de adoptar medidas físicas y lógicas, para proteger el acceso a las instalaciones, a los medios y equipos donde se almacena, procesa o comunica la información.

l. El Oficial de Seguridad de la Información y el Comité de Seguridad de la Información, deben de poner en funcionamiento medidas para asegurar que los funcionarios, contratistas y demás colaboradores, comprendan sus responsabilidades, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información.

m. Los usuarios deben prever medidas para evitar o minimizar la posibilidad de que la información a su cargo sea copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

n. La GITE debe adoptar medidas para minimizar la posibilidad de extracción de información o transmisión de virus informáticos, haciendo uso de dispositivos de almacenamiento externo (memorias USB, DVD, CD, Tablet, laptop, celulares, etc.).

o. La GITE debe mantener la seguridad de la información digital a la que tienen acceso instituciones externas o que son procesados, comunicados o dirigidas por estas.

p. La GITE debe de adoptar medidas para garantizar que el software empleado cumpla con las exigencias legales y de licenciamiento.

q. La GGC debe realizar auditorías del sistema de gestión de seguridad de la información, para verificar cumplimiento de objetivos, controles, políticas, planes, procedimientos de seguridad de la información.

r. Los Gerentes, Subgerentes, Jefes, deben verificar y supervisar el cumplimiento de las medidas de seguridad de la información en su área de responsabilidad.

s. La SG, GITE, GCRC (según competencias), deben proteger la información de la ONPE, por medio de medidas que evidencien uso adecuado de mensajeros, de mensajería instantánea y de redes sociales.

t. El Oficial de Seguridad de la Información, el Comité de Seguridad de la Información y la GCPH, deben determinar medidas disciplinarias para los servidores y funcionarios que hayan violentado la seguridad de la información institucional.

u. Los representantes de la ONPE en las ORC, ODPE así como en las oficinas distritales, deben de comunicar lo siguiente:

   (1) A la GOECOR, información sobre la coyuntura social o política de su jurisdicción.

   (2) A la OSDN, los reportes de incidentes de seguridad (según formato), así como, cualquier situación que pueda poner en riesgo la seguridad

de su sede y del proceso electoral, con la finalidad de que se adopten las medidas que resulten pertinentes.

v. La OSDN de la ONPE, efectuará las coordinaciones con las FFAA, PNP y de ser necesario con otras Instituciones, para prever acciones de seguridad que faciliten el normal desarrollo del proceso electoral.

w. Los jefes de las ODPE y gestores de las ORC reforzarán las coordinaciones con las FFAA, PNP y otras instituciones (según corresponda), en cada una de sus jurisdicciones como parte de las acciones preventivas de seguridad.

Las reuniones de coordinación de seguridad quedarán evidenciadas en actas (según formato elaborado por la OSDN).

x. Los jefes de las ODPE y gestores de las ORC deben disponer de un directorio con el nombre de las personas e Instituciones de apoyo, con las que además deben mantener buenos niveles de comunicación y de coordinación.

y. Los jefes de las ODPE deben además identificar los peligros y evaluar los riesgos a los que están expuestos el personal, la instalación, los bienes e información a su cargo, a fin de adoptar las medidas que correspondan, esta acción puede ser coordinada con la OSDN.

z. Los jefes de las ODPE deben adoptar las medidas de seguridad que correspondan a su realidad, tomando como base el presente Plan de Seguridad y siguiendo los lineamientos dados por la OSDN.

aa. GCPH, GOECOR, GITE, GGE, GIEE, OSDN deben determinar sus procesos críticos para darle el tratamiento de seguridad que requieren, considerar prioritariamente aspectos relacionados a: selección de personas, custodia de sedes institucionales y de los locales de votación, rutas para el despliegue y repliegue, protección de equipos y material electoral durante sus desplazamientos y almacenaje, custodia de equipos de voto electrónico y SEA, servicios de energía eléctrica, Internet, teléfono, agua, entre otros.

6.2 Fase de ejecución

De observarse algún peligro, vulnerabilidad o riesgo de seguridad, las instancias involucradas deben proceder de la siguiente manera:

a. Evaluar rápidamente la situación y en función al resultado coordinar con las instancias que correspondan para recibir el apoyo respectivo: OSDN, GOECOR, GITE, PNP, FFAA, MP, DP, Bomberos, Centros de Salud, DIVINDAT, COCIB, entre otros.

b. Proporcionar las facilidades para que las instituciones de apoyo puedan realizar sus labores sin inconvenientes.

c. Poner en práctica los Procedimientos Operativos de Seguridad (Anexo A).

6.3 Fase posterior

En esta fase, las instancias involucradas deben proceder de la siguiente manera:

a. Evaluar daños y adoptar medidas para controlarlos o minimizarlos.

b. Retomar las actividades previa indicación del personal autorizado.

c. Realizar las denuncias, reportes, informes que sean convenientes.

d. Efectuar la investigación de los acontecimientos suscitados, con la finalidad de identificar las causas básicas y adoptar las medidas de seguridad pertinentes.

e. Generar la documentación que corresponda.

f. Efectuar las coordinaciones necesarias con la OSDN.

VII. ACTIVIDADES OPERATIVAS Y ACCIONES DEL PLAN

Para el cumplimiento del presente plan se ha previsto el apoyo del CCFFAA y de la PNP (según competencias), de las empresas de seguridad y vigilancia contratadas para la custodia de los locales, así como, de las siguientes gerencias de la ONPE: OSDN, GOECOR, GITE, GIEE, GGE, GCRC, GCPH.

7.1 TAREAS ESPECÍFICAS

7.1.1 Comando Conjunto de las Fuerzas Armadas y Policía Nacional del Perú – CCFFAA / PNP

a. Protección de los funcionarios electorales durante el cumplimiento de sus labores.

b. Custodia, resguardo de los equipos, material, documentos y demás elementos destinados al desarrollo del acto electoral, seguridad en el despliegue del material electoral desde la ciudad de Lima hacia las oficinas descentralizadas de procesos electorales (ODPE) y desde estas hacia los locales de votación. Asimismo, durante el repliegue del material electoral desde los locales de votación hacia el centro de cómputo de la ODPE y posteriormente hacia el local que designe la ONPE.

c. Prestar el auxilio correspondiente que garantice el funcionamiento de las mesas de sufragio a solicitud de la ONPE.

d. Detener a ciudadanos en flagrante delito.

e. Mantener el libre tránsito del elector desde el día anterior de la votación y durante las horas de sufragio.

f. Impedir que haya coacción, cohecho, soborno, u otra acción que vulnere la libertad del elector.

g. A solicitud del Coordinador de Local de Votación de la ONPE o de los miembros de las mesas de sufragio, dar el apoyo que les compete para el normal funcionamiento de las mesas de sufragio en el interior del local de votación.

h. Facilitar el ingreso de los personeros a los locales donde funcionen las mesas de sufragio.

i. Custodia de los locales donde funcionen los organismos electorales.

j. Custodia de los locales de votación, antes, durante y después del proceso electoral (según coordinaciones efectuadas con la ONPE).

La custodia de los locales de votación concluye con el retiro total de los equipos y material electoral y previa comunicación con el coordinador del local de votación (Representante de la ONPE en el lugar).

k. Cumplir estrictamente lo prescrito en la cartilla de instrucción para las FFAA y la PNP elaborada y distribuida por la ONPE.

l. Asistencia, monitoreo, alerta, en asuntos relacionados a la Ciberdefensa, por medio del COCIB.

m. Apoyo en la investigación de delitos informáticos, por medio de la DIVINDAT.

7.1.2 Empresa de Vigilancia – EV

Protección de las sedes de la ONPE según bases integradas y Contrato.

7.1.3 Oficina de Seguridad y Defensa Nacional – OSDN

a. Coordinar con la PNP la custodia de las sedes de los actores electorales (JNE, RENIEC, ONPE, JEE, ORC, ODPE).

b. Coordinar con las FFAA y PNP la custodia de los locales de sufragio.

c. Coordinar el resguardo policial de los equipos y material electoral.

d. Coordinar con las Unidades Orgánicas de la entidad temas de seguridad de acuerdo a su competencia (GITE, GCPH, GGC, GCRC, GAD, GAJ, GSFP, GIEE, GPP, GG, SG, JN, GOECOR, GGE, OCI).

e. Realizar coordinaciones con instituciones para disponer de información que contribuya con el desarrollo del Proceso Electoral.

f. Realizar coordinaciones con instituciones que puedan apoyar en situaciones de emergencia durante los procesos electorales.

g. Capacitar al personal de GOECOR sobre aspectos de seguridad relacionados con: manejo de crisis, plan de seguridad, gestión del riesgo de desastres, matriz y mapa de riesgos electorales.

h. Emitir Oficios al CCFFAA, a la PNP u otras instituciones según corresponda, para coordinar acciones en favor de la seguridad de las ELECCIONES CONGRESALES EXTRAORDINARIAS 2020.

i. Elaborar la cartilla de instrucción para los efectivos de las FFAA y PNP.

j. Elaborar la cartilla informativa para los representantes del Ministerio Público.

k. Remitir a la PNP, FFAA y Ministerio Público las cartillas de instrucción e informativa para el referido proceso electoral

l. Elaborar y difundir el Plan de seguridad y otros documentos que fortalezcan la seguridad del proceso electoral.

m. Solicitar el resguardo policial para el desplazamiento (despliegue y repliegue) de personal, material y equipos electorales desde la Sede Central a las ODPE y viceversa.

n. Solicitar a la PNP y FFAA la custodia que se requiere para los locales de votación (interna y externa).

o. Recibir de la Gerencia de Gestión Electoral - GGE, la siguiente información:

- ✓ Las fechas previstas para el despliegue y repliegue de materiales y equipos electorales.
- ✓ El itinerario y cronograma de despliegue y repliegue indicando las rutas programadas e información de variables externas como: condiciones climáticas, interrupción de vías de comunicación, entre otras que guarden relación con la seguridad del desplazamiento de materiales y equipos electorales.
- ✓ Información de los comisionados y choferes: nombres, DNI, teléfonos, así como, las características de las unidades móviles que utilizarán (tipo, placa, color, etcétera).
- ✓ La información descrita debe ser proporcionada con una anticipación máxima de 72 horas para facilitar las coordinaciones con la PNP y el CCFFAA.

p. Recibir de la GOECOR, la siguiente información:

- ✓ El reporte de la cantidad de locales de votación y mesas de sufragio por distrito, provincias, ODPE u ORC y departamento.
- ✓ El itinerario de despliegue y repliegue de equipos y material electoral desde las ODPE u ORC hacia los locales de votación y viceversa.

q. Remitir la información que requiera la PNP y FFAA a fin de que planifiquen las actividades de seguridad de su competencia.

r. Remitir los acuerdos al oficial de enlace de la PNP y del CCFFAA para su conocimiento y validación.

s. Coordinar con la PNP la asignación de patrulleros para resguardar los vehículos previstos para trasladar los equipos y material electoral.

t. Solicitar al CCFFAA, PNP, DP, PCM, JNE, entre otros, reportes socio políticos y de coyuntura social de las regiones y distritos donde habrá proceso electoral.

u. Coordinar con las instituciones pertinentes para obtener información que favorezca a la planificación de la seguridad del proceso electoral.

v. Proporcionar información de Defensa Civil a las unidades orgánicas de ONPE a fin de facilitar las labores de evacuación por emergencia.

w. Adoptar medidas para el control de ingreso de dispositivos móviles (teléfonos celulares, tabletas, laptop, cámaras fotográficas y de video, grabadores, entre otros).

x. Adoptar medidas para controlar el acceso de personas a las instalaciones y ambientes de la entidad, muy en especial a las áreas donde se maneja información crítica.

y. Coordinar con el Oficial de Seguridad de la Información y el Comité de Seguridad de la Información, asuntos relacionados a la seguridad de la información de la entidad.

z. Verificar, supervisar y controlar el cumplimiento de las medidas de seguridad de la información en su área de responsabilidad.

7.1.4 Gerencia de Organización Electoral y Coordinación Regional - GOECOR

a. Coordinar con la OSDN las medidas de seguridad que deben aplicar las ODPE y ORC en el marco de las ECE 2020.

b. El JODPE debe definir el medio (terrestre, aéreo, acuático) por el cual se realizará el despliegue, repliegue del material y equipo electoral desde las ODPE hacia los distritos, centros poblados y viceversa, y prever las acciones pertinentes para que estos desplazamientos se realicen sin inconvenientes, en coordinación con la GOECOR.

c. El JODPE debe formular, con apoyo de la PNP y CCFFAA, el diseño de las rutas definiendo la principal y la alterna, teniendo en consideración factores como: la situación político social que se presenta en cada distrito, conflictos sociales, zonas críticas de incidencia delictiva, marchas, bloqueos de vías, huelgas, siniestros, problemáticas del tránsito vehicular, etcétera, mencionado diseño debe formularse en consideración a los siguientes formatos:

   - ✓ FM01-GOECOR/DMS “Rutas y Medios de Transporte para el Despliegue de Equipos y Materiales Electorales”.
   - ✓ FM02-GOECOR/DMS “Rutas y Medios de Transporte para el Repliegue de Equipos y Materiales Electorales”.

d. El JODPE debe de adoptar medidas de seguridad, acordes a su realidad con la finalidad de estar preparados para atender contingencias y emergencias. Para ello, deben tener en cuenta el presente Plan de Seguridad, y los lineamientos establecidos por la OSDN.

e. El JODPE debe realizar reuniones con los oficiales de la PNP y FFAA (coordinadores de su región), y con los representantes de las entidades del sector público y privado (empresas que suministran energía eléctrica, INDECI, bomberos, MP, RENIEC, JEE, municipalidades, entre otros), a fin de tratar temas relacionados con la seguridad del proceso electoral. Las reuniones donde se aborden asuntos de seguridad, deben quedar evidenciadas en actas (según formato proporcionado por la OSDN para tal fin).

f. El JODPE debe mantener un buen nivel de comunicación con los oficiales designados por la PNP y CCFFAA, a fin facilitar las coordinaciones de seguridad que el proceso electoral exige.

g. El JODPE debe autorizar el inicio del despliegue y el repliegue del material de sufragio y equipos electorales solo si los efectivos de la PNP o de las FFAA acompañan su desplazamiento.

h. En caso que los efectivos de la PNP o de las FFAA. no lleguen para iniciar el despliegue o el repliegue, el JODPE se comunicará con el oficial PNP encargado de la coordinación, e inmediatamente informará de esta situación a la GOECOR y a la OSDN.

i. De presentarse problemas durante el despliegue y/o repliegue del material electoral, el JODPE se comunicará con el oficial coordinador de la PNP o FFAA, asimismo, informarán de esta situación a la GOECOR y a la OSDN, para las acciones pertinentes.

j. El Coordinador del local de votación debe aplicar las acciones previstas para el repliegue del material electoral una vez finalizado el escrutinio. Asimismo, debe verificar que el recojo y ordenamiento del material electoral, equipos informáticos, entre otros, se ejecuten con las medidas de seguridad correspondientes.

k. El personal designado de las ODPE para el repliegue del material electoral y de los equipos informáticos desde el local de votación hacia la sede de la ODPE, en caso se produzca bloqueo de las vías (sea por desastre natural o por conmoción social), deberá coordinar las acciones por seguir con los oficiales responsables de la PNP o de las FF.AA. que lo están custodiando, a fin de poner a buen recaudo al personal, material y equipos, informando sobre esta situación al JODPE quien informará a la GOECOR y a la OSDN.

l. Personal de la ODPE debe asegurarse que, durante el trayecto de repliegue del material electoral y equipos informáticos desde el local de votación hasta la ODPE, exista la custodia correspondiente.

m. El JODPE deberá comunicar al oficial PNP coordinador de la región, a la GOECOR y a la OSDN, el momento en que el material electoral y los equipos informáticos ya se encuentran en la ODPE, para la custodia respectiva.

n. El JODPE debe elaborar el plan de seguridad de su jurisdicción, siguiendo los lineamientos de la OSDN.

o. Difundir los documentos de seguridad a todas las instancias bajo su administración (Plan de Seguridad, información de Defensa Civil, entre otros)

p. Verificar, supervisar y controlar el cumplimiento de las medidas de seguridad de la información en su área de responsabilidad

7.1.5 Gerencia de Gestión Electoral - GGE

a. Formular y proponer a la Gerencia General los lineamientos necesarios para efectuar el despliegue y repliegue del material electoral (para capacitación, simulacro, sufragio y reserva) así como los procedimientos para el diseño, impresión, ensamblaje y contingencia.

b. Proporcionar a la OSDN la siguiente información:
   - Las fechas previstas para el desplazamiento del material y equipo electoral (impresión, preparación, capacitación, despliegue y repliegue).

- El itinerario y cronograma de despliegue y repliegue indicando las rutas programadas e información de variables externas como: condiciones climáticas, interrupción de vías de comunicación, entre otras que guarden relación con la seguridad del desplazamiento de materiales y equipos electorales.
- Información de los comisionados y choferes / nombres, DNI, teléfonos, así como, las características de las unidades móviles a emplearse (tipo, placa, color, etc., entre otros).
- La información descrita debe ser proporcionada con la debida anticipación, para facilitar las coordinaciones con la PNP y el CCFFAA.

c. Adoptar medidas para que las actividades que realiza la GGE en cumplimiento de sus funciones tengan la seguridad que este proceso electoral requiere, esto aplicaría para lo siguiente:

- Formular y proponer a la Gerencia General el contenido de los materiales electorales para ser utilizados en el sufragio (acta electoral, cédula de sufragio y formatos), así como el contenido de las ánforas de sufragio para el ensamblaje del material electoral.

- Elaborar el diseño y las especificaciones técnicas de los tipos de cédula de sufragio, actas electorales, formatos y cualquier otro material electoral, requerido para el desarrollo del proceso electoral. El diseño del acta padrón se proporcionará a la Gerencia de Informática y Tecnología Electoral – GITE.

- Efectuar el control de calidad de todo el material electoral durante el diseño, impresión, ensamblaje y despacho del mismo, incluido el acta padrón impreso por GITE.

- Ejecutar, supervisar y controlar el proceso de la impresión, ensamblaje y despacho del material electoral para sufragio y reserva, así como del material de capacitación y simulacro, así como las operaciones de despliegue y repliegue del material electoral en provincias hasta las Oficinas Descentralizadas de Procesos Electorales; y en Lima Metropolitana y Callao hasta los locales de votación.

d. Prever medidas para la custodia, buen uso y conservación del material electoral, en todos sus momentos: durante su elaboración, preparación, distribución, almacenaje, carga, descarga, despliegue, repliegue.

e. Prever medidas que aseguren la contratación de unidades móviles óptimas para el desplazamiento del material y equipos electorales, en perfecto estado de funcionamiento y con los repuestos y accesorios para atender oportunamente contingencias, reduciendo la posibilidad de accidentes y retrasos.

f. Autorizar el inicio del despliegue y el repliegue de los equipos y material electoral, solo si los efectivos de la PNP o FFAA acompañan el desplazamiento.

g. En caso que los efectivos de la PNP o de las FFAA no lleguen para iniciar el despliegue y el repliegue se deberá informar a los operadores del

centro de control y monitoreo del circuito cerrado de televisión de la OSDN.

h. La SGOE de la GGE realizará el monitoreo de los vehículos que transportan los equipos y materiales electorales, de presentarse alguna ocurrencia debe ser comunicada al Operador de CCTV de la OSDN.

i. Verificar, supervisar y controlar el cumplimiento de las medidas de seguridad de la información en su área de responsabilidad

7.1.6 Gerencia de Información y Educación Electoral – GIEE

a. Adoptar medidas para que las actividades que realiza la GIEE en cumplimiento de sus funciones cuenten con el grado de seguridad que el proceso electoral requiere, esto aplicaría para lo siguiente:

- Proponer y evaluar la capacitación para la ejecución del proceso electoral, dirigida a los trabajadores de la ONPE, personal contratado de las ODPE y actores electorales.
- Participar en la revisión de la información electoral de las campañas publicitarias que se transmiten a través de los medios masivos de comunicación, así como de los materiales electorales producidos por los órganos competentes.
- Emitir los lineamientos para dar el servicio de asistencia técnica en el proceso electoral a organizaciones políticas, instituciones públicas, privadas y organizaciones de la sociedad civil que lo soliciten.
- Elaborar, diseñar y diagramar las propuestas de material electoral y capacitación para las organizaciones políticas, instituciones públicas, privadas y organizaciones de la sociedad civil que lo soliciten en el marco del servicio de asistencia técnica y apoyo en materia electoral, de acuerdo a las posibilidades y recursos disponibles de la institución.

b. Realizar campañas de capacitación para miembros de mesa, personeros, Fuerzas Armadas, PNP, electores, respecto al proceso electoral.

c. Difundir información de seguridad (Plan de Seguridad, Defensa Civil, entre otros), en los programas de capacitación que realiza la GIEE en las ODPE.

d. Verificar, supervisar y controlar el cumplimiento de las medidas de seguridad de la información en su área de responsabilidad.

7.1.7 Gerencia de Informática y Tecnología Electoral - GITE

a. Adoptar medidas para que las actividades que realiza la GITE en cumplimiento de sus funciones tengan la seguridad que el proceso electoral requiere, esto aplicaría para lo siguiente:

- Velar por el funcionamiento, mantenimiento, licenciamiento, resguardo e inventario de todos los sistemas informáticos y de telecomunicaciones implementados en la entidad.

- Proporcionar el apoyo informático necesario a los diferentes órganos de la institución, entidades que conforman el sistema electoral, con respecto al tratamiento de la información relativa al proceso electoral.

- Proponer a la Gerencia General el procedimiento para la ejecución del sorteo de Miembros de Mesa, procesar y administrar los datos de los resultados del proceso electoral, administrar el sistema de control de la información de omisos y realizar la exclusión de los ciudadanos impedidos y exceptuados de ejercer el cargo de miembros de mesa.

b. Prever medidas de control para los sistemas informáticos por emplearse en la ELECCIÓN CONGRESAL EXTRAORDINARIA 2020 antes, durante y después del día de votación.

c. Prever los equipos para atender posibles contingencias que afectarían el normal desarrollo de los sistemas informáticos.

d. Efectuar las coordinaciones con las instancias que correspondan para tener el soporte técnico especializado que el proceso requiere.

e. Coordinar con el Oficial de Seguridad de la Información y el Comité de Seguridad de la Información, asuntos relacionados a la seguridad de la información digital e informática de la entidad.

f. Efectuar coordinaciones con el COCIB, con la finalidad de prever medidas que permitan atender aspectos relacionados a la Ciberseguridad y Ciberdefensa.

g. Efectuar coordinaciones con la DIVINDAT, con la finalidad de prever medidas que permitan atender aspectos relacionados con delitos informáticos.

h. Establecer roles, funciones, responsabilidades en la operación y administración de los sistemas informáticos de la ONPE, incluido teléfonos e impresoras.

i. Adoptar medidas para minimizar la posibilidad de extracción de información institucional o transmisión de virus informáticos, haciendo uso de dispositivos de almacenamiento externo (memorias USB, DVD, CD, Tablet, laptop, celulares, etc.).

j. Mantener la seguridad de la información digital de la entidad, a la que tienen acceso instituciones externas o que son procesados, comunicados o dirigidas por estas.

k. Adoptar medidas para garantizar que el software empleado por la entidad cumpla con las exigencias legales y de licenciamiento.

l. Establecer lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales.

m. Implementar herramientas para evitar la descarga de software no autorizado y códigos maliciosos en los equipos de la entidad, asimismo restringir el acceso a redes sociales, sistemas de mensajería instantánea, acceso a sistemas de almacenamiento en la nube y cuentas de correo.

n. Asesorar en la compra y aprobar todo aplicativo informático o software que usara la entidad.

o. Implementar controles criptográficos para la seguridad de la información digital de la entidad.

p. Prever medios de respaldo para garantizar la recuperación de la información y la infraestructura de software critica de la entidad, ante posibles fallas.

q. Emitir lineamientos para el uso adecuado de los correos electrónicos, el internet, las redes sociales, sin poner en riesgo la seguridad de la entidad.

r. Verificar, supervisar y controlar el cumplimiento de las medidas de seguridad de la información en su área de responsabilidad.

7.1.8 Gerencia de Comunicación y Relaciones Corporativas – GCRC

a. Adoptar medidas para que las actividades que realiza la GCRC en cumplimiento de sus funciones posean el grado de seguridad que proceso electoral requiere, esto aplicaría para lo siguiente:

- Supervisar la difusión y promoción de la comunicación que recibirá la ciudadanía respecto al proceso electoral.
- Diseñar, coordinar y ejecutar las actividades de protocolo del proceso electoral (sorteo de ubicación de organizaciones políticas en la cédula de sufragio, en la franja electoral, asignación de número de las organizaciones políticas locales y otros establecidos en las leyes vigentes).
- Conducir las acciones de comunicación y de relaciones públicas con los medios de prensa nacional e internacional, coordinando notas de prensa, comunicados oficiales, entrevistas, informes, reportajes, redes sociales, ONPE TV, entre otros.
- Proponer el diseño y organización del sistema de difusión de la votación desde el inicio del escrutinio electoral.
- Coordinar y supervisar la publicación de los resultados del sorteo de miembros de mesa en un medio de comunicación y en la página web institucional.

b. Recibir información actualizada por parte de la OSDN, GOECOR, GGE, GIEE y otros órganos de la ONPE sobre hechos relevantes en el marco de las ECE 2020.

c. Proporcionar información y resultados electorales en coordinación con los órganos que requiera informando sobre el cómputo de las mesas.

d. Adoptar medidas físicas y lógicas, para proteger el acceso a los ambientes, medios y equipos que poseen información crítica.

e. Establecer lineamientos para que la información institucional autorizada a difundir por el portal de la ONPE, redes sociales u otros, este debidamente verificada y respete los principios de confidencialidad, integridad y disponibilidad.

f. Verificar, supervisar y controlar el cumplimiento de las medidas de seguridad de la información en su área de responsabilidad

7.1.9 Gerencia Corporativa de Potencial Humano – GCPH

a. Los procesos de selección del personal administrativo y operativo que requerirá la ONPE para el proceso electoral, se ceñirán en estricto a las Directivas vigentes que sobre el particular ha elaborado la entidad.

b. Verificar, supervisar y controlar el cumplimiento de las medidas de seguridad de la información en su área de responsabilidad.

c. La Secretaría Técnica de Procedimientos Administrativos Disciplinarios de la GCPH efectuará las indagaciones para determinar si amerita la apertura de un proceso disciplinario a los servidores y funcionarios que podrían haber violentado la seguridad de la información institucional.

7.2 COMANDO Y COMUNICACIONES

7.2.3 COMANDO

La ejecución del presente plan se efectuará bajo la dirección de la Oficina de Seguridad y Defensa Nacional de la ONPE.

7.2.4 COMUNICACIONES

Para las comunicaciones que resulten pertinentes realizar se deberá tomar en cuenta los procedimientos establecidos en el Anexo A, así como las instancias que se mencionan a continuación:

a. Jefatura Nacional

b. Oficina de Seguridad y Defensa Nacional

c. Gerencia de Organización Electoral y Coordinación Regional

d. Gerencia de Informática y Tecnología Electoral

e. Gerencia de Gestión Electoral

f. Gerencia de Información y Educación Electoral

g. Gerencia de Comunicaciones y Relaciones Corporativas

h. Gerencia Corporativa de Potencial Humano

i. Oficinas Descentralizadas de Procesos Electorales

j. Oficinas de Coordinación Regional

k. OSDN del Reniec

l. Oficina de Seguridad del JNE

m. Oficial enlace del CCFFAA

n. Oficial enlace de la PNP

o. Regiones Policiales

p. Regiones Militares

q. División de Investigaciones de Delitos de Alta Tecnología

r. Comando Operacional de Ciberdefensa

s. Equipo de Respuesta ante Incidente de Seguridad Digital – PCM - PECERT

7.3 ADMINISTRACIÓN Y LOGÍSTICA

a. Del Personal

Elementos Propios

- ✓ Jefe de la ONPE, Manuel Cox Ganoza
- ✓ Gerente de la OSDN, Walter Iglesias Arévalo
- ✓ Gerente de la GOECOR (e), María Elena Tillit Roig
- ✓ Gerente de la GITE, Roberto Puyo Valladares
- ✓ Gerente de la GGE (e), María del Pilar Biggio Pastor
- ✓ Gerente de la GIEE, María del Pilar Biggio Pastor
- ✓ Gerente de la GCRC, Milagros Judith Vargas Fierro
- ✓ Gerente de la GCPH, Leslie Pacheco Herrera

b. Personal FFAA Y PNP

- ✓ General de División EP Cesar Augusto Astudillo Salcedo, Jefe CCFFAA
- ✓ Coronel EP Fidel Enrique Bocanegra Burga – CCFFAA
- ✓ Comandante EP Jhon Verde Bardales – CCFFAA
- ✓ Teniente General PNP José Luis Lavalle Santa Cruz, CGPNP
- ✓ Coronel PNP Victor José Zanabria Angulo – SCGPNP
- ✓ Coronel PNP Manuel Marcelo Centeno Rosales – SCGPNP
- ✓ Coronel Alejandro Díaz Changanaqui - DIVINDAT–PNP
- ✓ General FAP Augusto García Calderón – COCIB
- ✓ General EP Ernesto Castillo Fuerman - COCIB

c. Elementos de Apoyo

- ✓ Compañías de Bomberos
- ✓ Serenazgo
- ✓ Gobiernos Locales
- ✓ Gobiernos Regionales

- ✓ Regiones Policiales
- ✓ DIRIN
- ✓ Comisarías
- ✓ UDEX
- ✓ Policía de Tránsito
- ✓ Regiones Militares
- ✓ Presidencia de Consejo de Ministros
- ✓ Defensoría del Pueblo
- ✓ PROVIAS NACIONAL
- ✓ Centros hospitalarios
- ✓ Empresas eléctricas
- ✓ Empresas de agua
- ✓ Equipo de Respuesta ante Incidente de Seguridad Digital – PCM – PECERT.
- ✓ COCIB
- ✓ DIVINDAT

	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 Seguridad de ECE 2020-Versión 00**

2. ORGANO RESPONSABLE: **OSDN**

3. 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		Oct	Nov	Dic	Ene	Feb	Mar
III	**PROCESOS DE SOPORTE**												
3.7	**PROCESO: GESTIÓN DE LA SEGURIDAD INSTITUCIONAL**												
3.7.1	**ACTIVIDAD: Coordinación e inducción para la seguridad institucional**												
3.7.1.1	Coordinaciones con los organismos del sistema electoral, para compartir información y atender su necesidad de seguridad	OSDN	Reporte	Reporte	22/10/2019	30/01/2020	4	1	1	1	1		
3.7.1.2	Coordinaciones con entidades del Estado que coadyuven a la seguridad del proceso electoral	OSDN	Reporte	Documento	22/10/2019	30/01/2020	4	1	1	1	1		

3. 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		Oct	Nov	Dic	Ene	Feb	Mar
III	**PROCESOS DE SOPORTE**												
3.7	**PROCESO: GESTIÓN DE LA SEGURIDAD INSTITUCIONAL**												
3.7.1	**ACTIVIDAD: Coordinación e inducción para la seguridad institucional**												
3.7.1.3	Capacitar a los Jefes de ODPE y Coordinadores Administrativo en temas de seguridad	OSDN	Taller	Documento	25/10/2019	28/10/2019	2	2					
3.7.1.4	Capacitar a los Coordinadores de Capacitación de la GIEE en temas de seguridad en el día de la Jornada	OSDN	Taller	Documento	08/11/2019	08/11/2019	1		1				
3.7.1.5	Difundir el Plan de Seguridad ECE 2020 a las unidades orgánicas	OSDN	Documento	Documento	15/11/2019	15/11/2019	1		1				
3.7.1.6	Coordinar con la PNP, FFAA para el resguardo de equipos y material electoral durante sus desplazamientos	OSDN	Reporte	Reporte	22/10/2019	28/02/2020	5	1	1	1	1	1	

3. 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		Oct	Nov	Dic	Ene	Feb	Mar
III	**PROCESOS DE SOPORTE**												
3.7	**PROCESO: GESTIÓN DE LA SEGURIDAD INSTITUCIONAL**												
3.7.1	**ACTIVIDAD: Coordinación e inducción para la seguridad institucional**												
3.7.1.7	Coordinar con la PNP, FFAA para la custodia de los locales involucrados en el proceso electoral	OSDN	Reporte	Reporte	02/11/2019	25/01/2020	3		1	1	1		
3.7.1.8	Recibir y consolidar información de las ODPE para elaborar la Matriz de Riesgos Electorales	OSDN	Reporte	Reporte	02/11/2019	19/01/2020	3		1	1	1		
3.7.1.9	Elaborar y difundir el Mapa de Riesgo Electoral de la ECE2020	OSDN	Documento	Documento	02/01/2020	20/01/2020	1				1		
3.7.1.10	Realizar el monitoreo del Plan de Seguridad ECE 2020	OSDN	Reporte	Reporte	02/11/2019	28/02/2020	4		1	1	1	1	
3.7.1.11	Elaborar el informe de evaluación del Plan de Seguridad ECE 2020	OSDN	Documento	Documento	01/03/2020	31/03/2020	1						1

VIII. PRESUPUESTO REQUERIDO

El presupuesto para la ejecución del presente Plan será el previsto conforme a lo aprobado mediante el Plan Operativo Electoral ECE 2020.

IX. MONITOREO Y EVALUACIÓN

El monitoreo se realizará de forma mensual en FM10- GPP/PLAN y evaluación se realizará en marzo de 2020 en el FM 11-GPP/PLAN y estará a cargo de la OFICINA DE SEGURIDAD Y DEFENSA NACIONAL.

X. ANEXOS

a) Anexo “A” Procedimientos Operativos de Seguridad

b) Anexo “B” Directorio Telefónico de Emergencia

c) Anexo “C” Brigadas de Emergencia

d) Anexo “D” Planos de Evacuación

e) Anexo “E” Información de la ODPE u ORC

f) Anexo “F” PR01-OSDN/SP Seguridad del Proceso Electoral

g) Anexo “G” IN01-OSDN/SP Seguridad en el despliegue y repliegue

h) Anexo “H” IN02-OSDN/SP Acciones de contingencia para problemas durante el despliegue y repliegue del material de sufragio

i) Anexo “I” FMO1-OSDN/SP Formato de Acta Reunión de coordinación para el proceso electoral.

j) Anexo “J” OD01-OSDN/SP Acciones por implementar para prevenir y atender contingencias por emergencias y desastres en las sedes de las ODPE y ORC.

k) Anexo “K” OD02-OSDN/SP Ocurrencias de Conmoción Social.

l) Anexo “L” DI04-GGC/GC Lineamientos de Seguridad de la Información.

ANEXO A

PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD

POS 01 - CONTRA INTRUSIÓN

1. Prever medidas que regulen el control de acceso de personas (servidores, visitas, proveedores, periodistas, autoridades, entre otros), a pie o en vehículo, de manera que se cumpla con la identificación, revisión, registro, autorización. Aplicar la Directiva DI 01-OSDN/SI V00 “Control de Acceso a las sedes de la ONPE”.

2. Toda visita debe ser acompañada durante su ingreso y salida, para minimizar la posibilidad que transite por áreas no autorizadas.

3. Todo el personal (servidores, visitas, proveedores, periodistas, autoridades, entre otros), que ingresa a las sedes tiene que mostrar su credencial o pase de visita a la altura del pecho, para facilitar los controles de seguridad.

4. Prever el empleo de medios (talento humano, tecnología), que faciliten la observación de personas que estén merodeando por los alrededores de sus sedes.

5. Verificar:

    a. Estado de las instalaciones, muy en especial de la parte perimétrica (paredes, puertas, ventanas, techos, entre otros), para detectar facilidad de intrusión por estos lugares.

    b. Seguridad de las áreas internas que contienen bienes e información de valor.

    c. Operatividad de los dispositivos de seguridad.

6. El personal de seguridad no permitirá el ingreso de personas que presenten signos de haber ingerido licor o consumido estupefacientes.

7. El personal de seguridad no permitirá el acceso de personas que porten armas, a excepción del personal que, por razones de trabajo en las sedes electorales, están autorizadas.

8. Toda persona que incumple el procedimiento de control de accesos o que sea considerada sospechosa o que cometió intrusión, debe ser reportada a seguridad, a la PNP, a las FFAA, para la intervención correspondiente.

9. Todo servidor de los organismos electorales tiene la obligación de colaborar con el presente procedimiento.

POS 02 - CONTRA LA TOMA DE LOCAL

1. Prever y organizar los medios disponibles (talento humano, tecnología), para detectar oportunamente: concentración de personas, manifestaciones, disturbios y otras situaciones que podrían afectar la seguridad de la sede, a fin de adoptar medidas que minimicen la posibilidad de toma de local.

2. Ante la posibilidad de toma de local, proceder de la siguiente manera:
   a. Solicitar apoyo a la PNP o FFAA.
   b. Colocar las barreras físicas en la parte externa de la sede (si las hubiera).
   c. Cerrar las puertas de acceso a la instalación.
   d. Comunicar los hechos a la GOECOR y OSDN.

3. Prever la organización y funciones del personal para el manejo de crisis.

4. Dar las facilidades a la PNP y FFAA para que procedan de acuerdo a sus competencias.

5. Los servidores deben permanecer en sus ambientes de trabajo evitando cualquier tipo de contacto o exposición.

6. El personal de seguridad, a través de los medios disponibles (personas, circuito cerrado de televisión, entre otros), observará la situación a fin de ir midiendo la gravedad del evento, y en función a ello, efectuar las coordinaciones que resulten convenientes (reportes, solicitud de refuerzo de seguridad, etcétera).

7. El personal no debe salir del local para evitar poner en riesgo su integridad física, esta situación puede variar si peligra la vida, previa evaluación y determinación de evacuar.

8. Efectuar los reportes respectivos.

POS 03 - CONTRA ROBO

1. El robo puede tener como protagonistas a personas de la institución, extraños o ambos actuando en forma coludida.

2. Adoptar medidas en favor de la seguridad, delimitando responsabilidades de los bienes patrimoniales. Asimismo, emitir directivas para el cuidado de los bienes de poco volumen, dinero, documentos y artículos personales.

3. Para minimizar la existencia de este riesgo es muy importante hacer una adecuada selección de personal, verificar y asegurarse que las condiciones de seguridad de los ambientes sean adecuadas y controlar accesos y salidas de personas, vehículos y material en general.

4. El personal de seguridad y vigilancia o a quien se designe (por falta de este servicio), adoptará las siguientes medidas:

   a) Estricto control durante los ingresos y salidas de personas, vehículos, equipos, material en general, bienes personales, bienes patrimoniales y desechos.

   b) Todo movimiento de bienes debe realizarse con la autorización correspondiente (escrita y visada por el funcionario competente).

   c) Detener, comunicar y poner a disposición de quien corresponda a todo aquel que sea sorprendido intentando sustraer algún bien, enseres o artículos diversos.

   d) Efectuar el informe respectivo.

5. Efectuar la denuncia ante la autoridad policial y dar las facilidades para las investigaciones pertinentes.

POS 04 - CONTRA ASALTO

1. El asalto puede ser realizado por:

   a. Personal propio o coludido para la ejecución del delito.
   b. Personas que ingresan a las sedes, sorprendiendo los controles de seguridad, haciéndose pasar como visitas, contratistas, proveedores, trabajadores de servicios públicos, miembros de la PNP, FFAA, entre otros.

2. Reportar a las instancias pertinentes (PNP, FFAA, OSDN), la presencia de personas y de vehículos, sospechosos. Tener a la mano los teléfonos de Emergencia.

3. Priorizar la seguridad en la puerta de acceso a la instalación y los amientes considerados críticos.

4. Implementar dispositivos de alerta (timbre, alarma, luces).

5. Dar las facilidades al personal policial o de las FFAA quien se acercará al lugar a fin de evaluar la situación y efectuar la intervención, si el caso lo amerita.

6. Si no se contó con el apoyo oportuno de las FFAA o PNP y los controles fueron superados siendo el asalto inminente, actuar con prudencia e inteligencia, no exponerse, de ser posible observar características físicas de los asaltantes u cualquier otro detalle importante.

7. Superada la crisis se redactarán los informes pertinentes, y se denunciará el hecho ante la delegación policial correspondiente.

   En ningún caso se suplantarán las funciones o facultades policiales.

POS 05 - CONTRA DISTURBIOS

1. Utilizar los recursos disponibles (talento humano, tecnología, entre otros), para observar las inmediaciones de las sedes, a fin de detectar situaciones que podrían terminar en disturbios.

2. Reportar al personal de seguridad, a la OSDN, PNP y FFAA a fin de que proporcionen el apoyo correspondiente.

3. Bajo ninguna circunstancia se debe agredir (verbal o físicamente) a los manifestantes. El control del disturbio estará a cargo de la Policía o las FFAA.

4. El personal de seguridad debe registrar los disturbios por medio de fotos o filmaciones (sin exponerse), las que presentará como documentos adjuntos al informe que corresponde redactar.

5. Las sedes deben de cerrar sus puertas frente a disturbios.

6. Los servidores deben permanecer en el interior de las instalaciones hasta que se determine que pueden salir.

7. Elaborar el informe respectivo.

POS 06 - CONFLICTOS SOCIALES

1. Informarse de las asambleas, reuniones y acuerdos de gremios y otros actores sociales.

2. Recabar información sobre posibles marchas, paros, protestas.

3. Recabar información de los actores políticos y sociales.

4. Compartir información sobre la situación socio política de la zona, con la PNP, FFAA, DP, JNE, RENIEC, entre otros.

5. De presentarse el conflicto en las inmediaciones de la sede, adoptar medidas de seguridad externas (solicitar apoyo PNP, FFAA), o internas (cerrar puertas, no salir de la sede, no tener contacto con la población involucrada en el conflicto, no exponerse).

6. Si se encuentra fuera de la sede, refugiarse en un lugar seguro.

7. Evaluar el impacto de los hechos

8. Informar

POS 07 - CONTRA ATENTADOS TERRORISTAS

1. Efectuar una adecuada selección del personal.

2. Establecer controles de seguridad exhaustivos para el ingreso de personas, vehículos, bienes, equipos y materiales en general.

3. Reportar a la PNP, FFAA la presencia de personas, vehículos, paquetes sospechosos, para el apoyo e intervención correspondiente, quienes tomarán el control de las acciones. La observación resulta importante para este cometido.

4. Restringir accesos a las áreas críticas (centros de cómputo, archivos, almacenes de equipos y material electoral, entre otros).

5. Inspeccionar los ambientes a fin de detectar paquetes, bolsos, explosivos u otros.

6. Dejar que los especialistas manejen la situación, dé facilidades, no sea un obstáculo.

7. Evaluar la necesidad de evacuar la instalación.

8. Efectuar el informe respectivo.

POS 08 - CONTRA ACCIDENTES DE TRÁNSITO

1. Si es conductor, manejar respetando las normas de tránsito.
2. Evitar distracciones cuando maneje.
3. Si va a conducir no consuma bebidas alcohólicas.
4. Utilizar elementos de seguridad (triángulo, conos, cuñas, etcétera).
5. Ceder el paso a los peatones.
6. Ser cuidadoso al entrar o salir de estacionamientos.
7. Si es peatón observar con atención los lugares por donde transite, no distraerse, respetar los semáforos y las señales de tránsito.
8. Mantener su vehículo en perfecto estado, a fin de evitar accidentes por fallas de alguno de sus sistemas.
9. No desplazarse ni contratar medios de transporte público que no ofrecen garantía.
10. Observar las condiciones meteorológicas adversas.
11. Elegir las mejores rutas - vías de transporte.
12. Utilizar siempre las aceras y cruces peatonales.
13. Ser precavido en los paraderos de transporte público.
14. Colaborar con el procedimiento policial establecido para la atención de accidentes de tránsito.

POS 09 - CONTRA AGRESIONES FÍSICAS

1. No responder las agresiones físicas.

2. Tratar de identificar a los agresores, recordar circunstancias, características del lugar, testigos, entre otros lo cual ayudará en la investigación policial.

3. Efectuar la denuncia ante la PNP.

4. Acudir al médico legista.

5. Si la policía se niega a recibir la denuncia, es decir no cumple con sus funciones, se debe presentar la denuncia ante:
   a. La Inspectoría General de la Policía Nacional, las Inspectorías Regionales o las Oficinas de Disciplina Policial.

   b. El Ministerio del Interior, línea gratuita 1818, opción 3.

   c. La Defensoría del Pueblo o llamar a la línea gratuita 0800-15-170.

4. Si la agredida es mujer, se le derivará a un Centro de Emergencia Mujer para que los especialistas ejecuten las acciones conforme a los procedimientos aprobados por el Ministerio de la Mujer y Poblaciones Vulnerables.

5. Realizar el reporte o informe respectivo.

POS 10 - EXTORSIÓN

1. Identificar el método de extorsión (teléfono, mensaje de texto, una nota, redes sociales, artefacto que causa temor).

2. Mantener las pruebas de la extorsión. No borrar los mensajes, evitar manipular el celular o cambiar de número. Si la extorsión fuera por una llamada telefónica, mantenga la calma y ponga énfasis en el lenguaje del agresor.

3. Llamar a la policía (105 o al número que corresponde a su jurisdicción).

4. Acercarse a efectuar la denuncia para dar detalles que permitan identificar a los delincuentes.

5. Un punto importante, si realiza la denuncia por extorsión dentro de las 24 horas siguientes, la policía puede hacer una geolocalización del teléfono del extorsionador.

6. Es conveniente:

   - Mantener a buen recaudo la información confidencial.
   - No comunicar su número personal a cualquier persona.
   - Tener mapeado a los servidores, saber dónde viven, teléfonos y datos de familiares, esta información puede ser útil a la policía.
   - Actualizar la base de datos.
   - Hacer uso de sistemas de seguridad electrónicos.
   - Seleccionar bien a los colaboradores y darles información sobre este delito.

7. Reportar e informar.

POS 11 – CORRUPCIÓN

1. Realizar una adecuada selección de personal.
2. Identificar los puestos críticos, especialmente aquellos que manejan información sensible que puede ser objeto de corrupción.
3. Establecer controles internos.
4. Observar y evaluar comportamientos, conductas del personal.
5. Asumir el liderazgo.
6. Informar, capacitar, educar.
7. Intervenir.
8. Denunciar.
9. Elaborar el informe dando cuenta del hecho.

POS12 - INFIDENCIA

1. Comete infidencia toda persona que sin autorización se apropie, destruya, divulgue, facilite información clasificada o de interés institucional, que manifiestamente perjudique o ponga en grave peligro la seguridad del proceso electoral.

2. El funcionario que emita un documento tiene la responsabilidad de asignarle la categoría de seguridad que le corresponde, estableciendo su importancia en relación con la seguridad institucional.

3. El material crítico usado en el trabajo está considerado como Información Secreta, por tanto, debe ceñirse a todas las disposiciones correspondientes a esta categoría.

4. En lugares públicos o alrededor de personas desconocidas evite hablar sobre asuntos laborales.

5. Realizar una adecuada selección de personal.

6. Establecer controles para el acceso, manejo, distribución y destrucción de la información (digital e impresa).

7. No dejar al alcance de cualquier persona: documentos, CD, USB y otros. Si estos contienen información relacionada al trabajo y por alguna razón requiere retirarlos necesariamente debe contar con la autorización respectiva.

8. Informar, capacitar, educar para minimizar la posibilidad de que el personal incurra en este delito.

9. Observar comportamientos, conductas y efectuar la evaluación respectiva.

10. Intervenir.

11. Denunciar.

12. Elaborar el informe dando cuenta del hecho.

POS 13 - SABOTAJE

1. Siendo el sabotaje un proceso por el cual se realiza una modificación, destrucción, obstrucción o cualquier intervención en una operación ajena, no cabe duda que obedece a un interés subalterno que busca algún beneficio en particular.

2. El sabotaje puede tener origen interno o externo, por lo que corresponde adoptar medidas de control que ayuden a identificar circunstancias y personas involucradas.

   Dentro de estas medidas considerar como mínimo:

   a. Efectuar adecuados procesos de selección de personal.

   b. Establecer responsabilidades y funciones específicas a cada servidor.

   c. Designar a personal de confianza para los puestos considerados críticos.

   d. Mantener un buen clima laboral.

   e. Implementar acciones que permitan optimizar la seguridad de los ambientes, principalmente de aquellos que contienen bienes, equipos, información y material relevante (considerar sistemas tecnológicos de control de accesos, circuito cerrado de televisión, cerrojos, candados, estado de puertas, ventanas, paredes, techos, entre otros).

   f. Incidir en los controles de acceso, desde la calle hacia las sedes, así como al interior de las mismas, específicamente a las áreas consideradas críticas.

3. Efectuar las indagaciones correspondientes.

4. Efectuar la denuncia policial.

5. Informar.

POS 14 - INFILTRACIÓN

1. La infiltración es la técnica utilizada para introducirse en organizaciones para obtener información de interés inmediato o potencial sobre las actividades, capacidades, planes, proyectos, etcétera del contrario.

1. Realizar una buena selección de personal.

2. Verificar la información proporcionada por los servidores en su hoja de vida (estudios, domicilio, familia, experiencia laboral, referencias, teléfono, correo electrónico, entre otros).

3. Verificar antecedentes penales, policiales, judiciales.

4. Verificar que el personal no esté inscrito en algún partido político.

5. Determinar actividades, tareas, funciones, responsabilidades que debe asumir el servidor.

6. Especificar la información a la que tiene acceso cada servidor y establecer el grado de seguridad y responsabilidad que debe asumir.

7. Observar comportamientos, conductas, hacer la evaluación respectiva. Especial atención a: cumplimiento de obligaciones, actitud que evidencia en el trabajo, interés por obtener información que no es de su competencia, accesos a áreas no autorizadas, manejo de información.

8. Incidir en el control de acceso a las sedes y ambientes internos a fin de detectar, oportunamente, cualquier intento de ingreso sin contar con la autorización respectiva.

9. Intervenir.

10. Denunciar.

11. Reportar e informar.

POS 15 - ESPIONAJE

1. Siendo el espionaje la práctica o conjunto de técnicas asociadas a la obtención encubierta de datos o información confidencial y cuyo proceder se basa en la infiltración y la penetración, es pertinente adoptar medidas para detectar, neutralizar o actuar adecuadamente frente a este delito mediante el cual se soborna y chantajea.
2. La infiltración es la técnica utilizada para introducirse en organizaciones para obtener información de interés inmediato o potencial sobre las actividades, capacidades, planes, proyectos, etcétera, del contrario.
3. La penetración es la técnica que consiste en lograr la colaboración consciente o inocente de un miembro de la organización o grupo contrario con el fin de que proporcione datos e información confidencial. Generalmente, esta actividad se realiza de forma encubierta y emplea personas reclutadas que han sido persuadidas para trabajar en secreto en contra de su propia organización por diferentes motivaciones: ideológicas, económicas, morales, religiosas o personales.
4. Las acciones que deben aplicarse para atender este delito son:

    a. Hacer una buena selección de personal.
    b. Verificar la información proporcionada por los servidores en su hoja de vida (estudios, domicilio, familia, experiencia laboral, referencias, teléfono, correo electrónico, entre otros).
    c. Verificar antecedentes penales, policiales, judiciales.
    d. Determinar actividades, tareas, funciones, responsabilidades que debe asumir el servidor.
    e. Especificar la información a la que tiene acceso cada servidor y establecer el grado de seguridad y responsabilidad que debe asumir.
    f. Observar comportamientos, conductas, hacer la evaluación respectiva.
    g. Observar: cumplimiento de obligaciones, actitud que evidencia en el trabajo, interés por obtener información que no es de su competencia, accesos a áreas no autorizadas, manejo de información.
    h. Incidir en el control de acceso a las sedes y ambientes internos, a fin de detectar oportunamente cualquier intento de ingreso sin contar con la autorización respectiva.
    i. Intervenir.
    j. Denunciar.
    k. Reportar e informar.

POS 16 - CLIMA LABORAL NO ÓPTIMO

1. Promover el respeto.
2. Fomentar una efectiva comunicación.
3. Ejercer liderazgo.
4. Aplicar reconocimientos.
5. Disponer de un lugar de trabajo adecuado.
6. Incentivar, motivar.
7. Fomentar la transparencia, actitudes positivas.
8. Organizar, estableciendo y definiendo procesos y tareas,
9. Fomentar el trabajo en equipo.
10. Reportar e informar.

POS 17 - INTERRUPCIÓN DEL FLUIDO ELECTRICO

1. Encargar o revisar periódicamente las instalaciones eléctricas del local para garantizar que estén en buen estado.

2. Revisar periódicamente el estado del grupo electrógeno – G.E., hacer el mantenimiento y las pruebas respectivas para asegurar su operatividad.
   Si no se dispone de G.E., evaluar la necesidad de contar con este equipo y/o prever su alquiler.

3. Si se detecta conexiones en mal estado (cables, enchufes, interruptores, tomacorrientes, llaves, entre otros), coordinar su reparación o cambio inmediato.

4. Verificar o encargar la revisión de cables, enchufes, de los equipos de cómputo o eléctricos en uso, a fin de asegurarse que estén en buen estado.

5. No sobrecargar las instalaciones eléctricas.

6. Disponer de linternas y luces de emergencia, verificar que se encuentren operativas.

7. De ser necesario, solicitar el apoyo de la empresa eléctrica responsable del sector.

8. Reportar e informar.

POS 18 - INUNDACIÓN

1. Revisar periódicamente las tuberías de agua y desagüe ubicadas en los ambientes de la sede.

2. Revisar permanentemente el estado de los techos que no son de concreto (calaminas, tejas, planchas plastificadas, etc.), a fin de detectar condiciones inseguras que pueden facilitar las filtraciones.

3. Prever la colocación de equipos y materiales en general sobre una base de por lo menos 15 cm. de altura, preferible de madera, para evitar el contacto directo con el suelo y el deterioro respectivo.

4. Proceder al corte del fluido eléctrico (haga uso de la llave principal).

5. Usar linternas de mano para la inspección de los ambientes.

6. Desplazar el mobiliario, los equipos y el material electoral afectado a otros ambientes más seguros y secos.

7. Iniciar el retiro de las aguas empozadas con los medios disponibles. De ser necesario, solicitar apoyo de los Bomberos o de la empresa de agua y desagüe del sector.

8. Activar las brigadas de emergencia.

9. Coordinar se brinde los primeros auxilios, de ser necesario.

10. Evaluar daños y con la ayuda de INDECI determinar si el local es habitable.

11. Revisar las instalaciones eléctricas a fin de verificar su funcionamiento.

12. Revisar cuidadosamente los equipos que estuvieron expuestos al agua, a fin de evitar o producir su mal funcionamiento en caso de ser encendidos.

13. Si existe documentación y/o material electoral húmedo, para su recuperación, se deberá:
    a. Ubicar la documentación en ambientes amplios, ventilados y secos.
    b. Proceder al secado manual
    c. Separar, los documentos manchados de barro y limpiarlos.

14. Informar.

POS 19 - EMERGENCIAS POR SALUD

1. Mantener la calma.
   Evitar comentarios con otras personas y abstenerse de dar diagnósticos de cualquier naturaleza que resulten contraproducentes.
   De ser posible identificar a la persona que presenta la emergencia y a sus acompañantes.

2. Evitar aglomeraciones.

3. No mover al herido, sobre todo si se trata de fracturas (los movimientos pueden complicar su estado de salud), salvo que su condición requiera urgente traslado.

4. Examinar al herido. Atenderlo y estar a cargo de él hasta que pueda ser confiado a personas calificadas, o hasta que se recupere o esté en manos de sus familiares.

5. Planificar las acciones a seguir, teniendo en cuenta el tipo de accidente o enfermedad generada.

6. Tranquilizar al herido, manteniendo frente a él la serenidad debida, evitando crear pánico y zozobra.

7. Mantener la temperatura.

8. Solicitar ayuda a los servicios de emergencia, para que personal especializado se haga cargo de la situación.

9. Trasladar en forma adecuada, para recibir atención especializada.

10. No medicar, utilizar sólo las medidas y técnicas apropiadas para brindar los primeros auxilios. Además, no deben realizar maniobras forzadas que puedan causar daños irreparables.

11. El que presta los primeros auxilios no debe extralimitarse más allá de sus conocimientos y capacidad.

12. Reportar e informar.

POS 20 - SISMO

1. Brindar información y capacitación sobre sismos.
2. Identificar y señalizar las áreas internas y externas, zonas de peligro, rutas de evacuación y zonas de seguridad.
3. Las rutas de evacuación deben estar libres para facilitar la evacuación.
4. Tener a la vista el directorio telefónico de emergencia y la mochila de emergencia con los implementos sugeridos por INDECI.
5. Realizar simulacros frecuentes de evacuación. Reunir al personal y revisar medidas de seguridad.
6. Organizar la evacuación. Activar las brigadas de emergencia.
7. Evacuar a las zonas de seguridad con serenidad, orden, mantener la calma, no correr desesperadamente, no gritar; estas actitudes contagian y desatan el pánico.
8. Si el sismo ocurre de noche utilice linternas a pilas para alumbrarse, nunca fósforos, velas o encendedores.
9. Si se encuentra conduciendo un vehículo, deténgase y permanezca dentro de él, alejándose de árboles, postes de alumbrado y letreros.
10. Si el sismo lo sorprende en la costa, aléjese de las playas, podría ocurrir un maremoto o tsunami.
11. Mantenerse alejado de los precipicios y riberas de los ríos.
12. Prepararse para las réplicas, no retornar a sus viviendas.
13. Si está capacitado, apoyar con primeros auxilios y llamar a personal médico.
14. No caminar descalzo, podría pisar vidrios u objetos cortantes.
15. Coordinar acciones con los representantes del INDECI y otorgar las facilidades que requieran.
16. Reportar e informar usando los medios más idóneos.

POS 21 - INCENDIO

1. Evitar la acumulación de basura.
2. Evitar la sobrecarga de tomacorrientes.
3. Evitar el uso de cables eléctricos parchados, viejos o deteriorados.
4. Mantener orden y limpieza.
5. Mantener los ambientes debidamente ventilados.
6. No acumular material inflamable.
7. Guardar los líquidos inflamables en lugar seguro.
8. Distribuir adecuadamente los equipos de extinción de incendios.
9. Colocar señalización de seguridad.
10. Capacitar al personal sobre incendio y forma de combatirlo.
11. Realizar simulacros de incendio.
12. Si está capacitado para extinguir un amago de incendio, hágalo, adopte las medidas de seguridad respectivas.
13. Comunicar a los Bomberos, Defensa Civil y la PNP.
14. Evaluar daños.
15. Rescatar la documentación y/o material electoral.
16. Reunir al personal y reforzar las medidas de seguridad.
17. Recargar los extintores empleados.
18. En caso de quemadura, lavar la parte afectada con agua fría y limpia. No reventar las ampollas.
19. No desprender trozos de ropa adheridos a las quemaduras.
20. Retorne a las instalaciones si las autoridades confirman que no hay peligro.
21. Seguir instrucciones de los Bomberos o Representantes de Defensa Civil.

POS 22 – TSUNAMIS

1. Conocer las zonas de seguridad establecidas y las rutas de evacuación.
2. Si está cerca de la playa, evacuar hacia las zonas de seguridad después de que haya ocurrido un sismo de gran intensidad llevando su equipo de emergencia.
3. Tener preparado su equipo de emergencia conteniendo un botiquín de primeros auxilios, radio a pilas, linterna, frazadas, fósforos, velas, etc.
4. Escuchar los boletines oficiales y retornar cuando las autoridades confirmen que no se producirá un Maremoto.
5. Evacuar a las zonas de seguridad en forma inmediata, seguir las rutas de evacuación establecidas, asegurarse que cada miembro lleve únicamente lo indispensable.
6. Recordar que la aproximación de un Maremoto es precedida normalmente por una subida o bajada (retirada) notable de las aguas en la costa.
7. Infundir serenidad y ayudar a la evacuación de niño, ancianos o impedidos.
8. El Comité de Defensa Civil de la comunidad realizará una evaluación de daños causados por el Maremoto.
9. Retornar a sus viviendas cuando el Comité de Defensa Civil lo autorice.
10. Mantenerse informado y escuchar los boletines emitidos por las autoridades de Defensa Civil.
11. Facilitar los trabajos de reconstrucción que realizará el Comité de Defensa Civil.
12. Hacer los reportes respectivos.

POS 23 - RIESGOS POR CONDICIONES CLIMATOLÓGICAS

1. Mantenerse informado de las condiciones climatológicas de la zona.

2. Tomar las previsiones de seguridad ante los pronósticos de frío, calor, lluvias, humedad, vientos, entre otros, a fin de evitar la presencia de enfermedades, accidentes, deterioro de bienes, equipos y/o materiales en general.

3. Mantener coordinación con las Instituciones del lugar encargadas de brindar apoyo ante condiciones climatológicas adversas.

4. Compartir información sobre las condiciones climatológicas del lugar, instruir, capacitar, para que las actividades se realicen adoptando las medidas de seguridad que corresponden.

5. Solicitar apoyo.

6. Reportar e informar.

POS 24 - EMBOSCADA

1. Mantener en estricta reserva información relacionada con los desplazamientos de personas, bienes y material en general: fechas, horas, rutas, medios de transporte.

2. Manejar códigos, claves, que dificulten comprender la información, en caso esta llegue a personas no autorizadas.

3. Mantenerse informado sobre el estado de las carreteras, de las vías de tránsito, por donde tiene previsto desplazarse.

4. Establecer rutas alternas y horarios.

5. Observar atentamente por donde se desplaza en vehículo, a fin de detectar posibles bloqueos de vías u otras estrategias para emboscarlo.

6. Tener a la mano los teléfonos de emergencia, solicitar apoyo.

7. Reportar e informar.

POS 25 - SECUESTROS

1. Ser consciente de la seguridad personal e institucional.
2. Evitar proporcionar información personal e institucional a personas no autorizadas.
3. Evitar transitar por lugares considerados peligrosos o que no conozca.
4. Caminar en sentido opuesto al tránsito de vehículos.
5. Comunicar sus actividades solo a personas de su absoluta confianza (fecha, horario, lugar, persona con quién se reunirá, entre otros).
6. Evitar dar a conocer su situación económica; bienes, joyas, cargo.
7. Distribuir su dinero en distintas cuentas bancarias; evite llevar consigo todas sus tarjetas de crédito o mucho dinero en efectivo.
8. Evitar difundir sus viajes y publicar su ubicación en tiempo real en las redes sociales.
9. Cambiar constantemente las rutas por las que transita diariamente.
10. Estar alerta mientras caminas o conduces; evita distraerte con tu teléfono celular.
11. Estar atento y examinar detalles de su entorno; si notas alguna actividad o persona sospechosa, repórtala inmediatamente a las autoridades.

Si usted es secuestrado:

1. Mantenga la calma.
2. No sea un informante fácil. Escuche, analice y responda.
3. Minimice su situación social y nivel económico.
4. No polemizar, no importa cuán razonables parezcan sus argumentos.
5. Evite mirar al secuestrador a la cara.
6. Cumpla con las instrucciones de los captores lo mejor posible.
7. Tome nota mentalmente de todos los movimientos, incluyendo el tiempo, direcciones, distancias, olores especiales y sonidos.
8. Cuando le sea posible, tome nota de las características de los captores, de sus hábitos, modos de hablar, de los contactos que hacen de sus gustos o disgustos.
9. Si requiere de un medicamento o tratamiento médico, indíquelo al secuestrador.

POS 26 – 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.

POS 27 – 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.

POS 28 – FUGA DE INFORMACIÓN FÍSICA

1. Sensibilizar al personal respecto a las buenas prácticas de protección de la información documentada.
2. Sensibilizar al personal respecto a los procedimientos establecidos para el control de acceso a las sedes ONPE.
3. Aplicar la Directiva DI01 – OSDN – SI "Control de Acceso a las Sedes ONPE".
4. Aplicar el Instructivo IN01 – OSDN - SI "Registro y Control del Sistema de Video Vigilancia de las sedes ONPE".
5. Aplicar los siguientes procedimientos operativos de seguridad:
    - CONTRA INTRUSIÓN (POS01).
    - CONTRA ROBO (POS 03).
    - EXTORSIÓN (POS 10).
    - CORRUPCIÓN (POS 11).
    - INFIDENCIA (POS 12).
    - INFILTRACIÓN (POS 14).
    - ESPIONAJE (POS 15).
6. Clasificar la información y disponer los controles respectivos.
7. Custodiar la información física bajo llave en armarios, gavetas, etc.
8. No abandonar la información física en las bandejas de las impresoras.
9. Restringir los accesos a los ambientes, áreas consideradas críticas.
10. Registrar a los visitantes que cuentan con autorización para ingresar a ambientes donde se almacena información física.
11. Restringir a los visitantes que ingresen a las sedes institucionales portando dispositivos móviles (teléfonos celulares, tabletas, laptop, USB, cámaras fotográficas y de video, grabadores, entre otros).
12. Los servidores de la entidad no deben hacer mal uso de la información institucional, en el mismo sentido, no deben compartirla si no cuentan con la autorización para hacerlo, bajo responsabilidad. Especial cuidado con el uso de celulares, USB, laptop, Tablet, cámaras fotográficas y de video, grabadores de audio, entre otros.
13. No entregar información física a personas no autorizadas.
14. Los servidores de la entidad no deben retirar equipos portátiles que contienen información institucional, sino cuentan con la autorización respectiva.
15. Al imprimir documentos con información que no tenga carácter público, deben ser retirados y no dejados sin custodia.
16. Reportar los incidentes donde se observe incumplimiento a las disposiciones relacionadas con la seguridad de la información.
17. Todo incumplimiento de las disposiciones de seguridad de la información dará lugar a la investigación pertinente para determinar las causas y los correctivos que correspondan.

ANEXO B

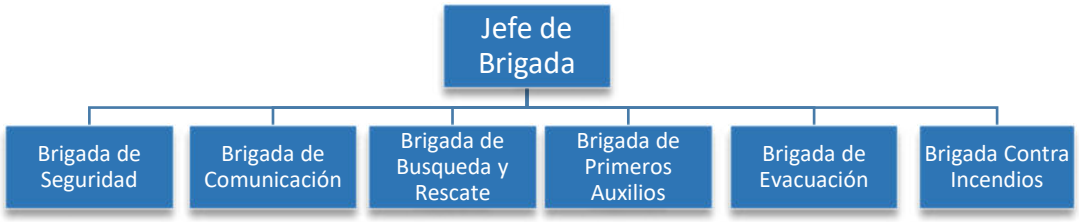
DIRECTORIO TELEFÓNICO (*)

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 función a la ubicación de cada sede a nivel nacional.

ANEXO C

ORGANIZACIÓN DE LAS BRIGADAS



Jefe de Brigadas

Antes:

- Planear la organización de las brigadas.
- Trazar planes de acción.
- Proveer lo conveniente para el entrenamiento y capacitación.
- Asignar tareas y responsabilidades a los miembros de las brigadas.

Durante:

- Coordinar las operaciones durante las emergencias.
- Motivar y mantener en alto la moral de las brigadas.

Después

- Consolida el informe final junto con los miembros de las brigadas.
- Entrega de informe final a la OSDN

Brigada de Seguridad

Antes:

- Recibir adiestramiento y práctica sobre las normas de seguridad.
- Mantener libres y despejados los accesos a las instalaciones.
- Reconocer las áreas seguras y de seguridad que empleará ONPE.

Durante:

- Apoyar en las labores de seguridad, minimizando la posibilidad de intromisión y otros.
- Ayudar a Identificar las áreas de mayor riesgo.
- Ayudar a clausurar las áreas que han sido evacuadas.

Después

- Revisar y mantener despejados los accesos a las instalaciones.
- Elaborar un informe de las actividades que son de su competencia.
- Entregar el informe completo a la OSDN.

Brigada de Comunicación

Antes:

- Recibir adiestramiento y práctica para saber cómo realizar su labor.
- Mantener la lista de números telefónicos de emergencia actualizado.

Durante:

- Realizar la comunicación con las entidades de emergencia.
- Establecer la red de comunicaciones que están implementados para atender la contingencia y la redirección según los resultados.

Después:
- Comunicar la orden de retorno seguro a las instalaciones, una vez superada la emergencia.
- Consolidar el informe final junto con las otras brigadas.
- Entrega de informe final a la OSDN

Brigada Búsqueda y Rescate

Antes:
- Recibir adiestramiento y práctica para saber cómo realizar el traslado de heridos y lesionados con el mínimo peligro para conservar su integridad física.
- Practicar diversas formas de rescate simulado en situaciones difíciles, asesorados siempre por personal técnico capacitado.
- Contar con el equipo mínimo necesario para rescatar a las personas atrapadas (camillas, sogas, picos, palas, etc.)
- Conocer y practicar las técnicas básicas para el rescate de una persona lesionada o atrapada en una contingencia.

Durante:
- Apoyar en sus labores a la brigada de evacuación.
- Permanecer al pendiente del pase de lista del personal evacuado.
- Identificar las áreas de mayor riesgo.
- Realizar de inmediato, si la emergencia lo permite, la búsqueda y rescate de lesionados.
- Clausurar las áreas que han sido desalojadas.
- Recibir el reporte, por parte de la brigada de evacuación, del personal ausente.

Después:
- Hacer recorridos a la zona de riesgo para determinar el fin de la emergencia.
- Pasado el riesgo, esta brigada deberá recorrer las instalaciones, para conocer el grado de afectación, delimitando la zona de riesgo y determinando si el inmueble es seguro para su ingreso.
- Informar en forma veraz y juiciosa al área de OSDN el suceso acaecido y el estado de las instalaciones, así como del personal.
- Elaborar un informe de las actividades realizadas y entregarlo a la OSDN.

Brigada de Primeros Auxilios

Antes:
- Tomar cursos de primeros auxilios; impartidos por personal especializado en el tema.
- Realizar prácticas continuas de atención de heridos, fracturas, vendajes, reanimación cardiopulmonar (RCP), etc.
- Tener un botiquín de primeros auxilios en lugares visibles y de fácil acceso, acorde con la actividad y los riesgos detectados.
- Revisar el contenido y caducidad de los medicamentos periódicamente.
- Contar con un directorio de los servicios médicos de apoyo interno y externo.
- Recibir capacitación periódicamente en técnicas de primeros auxilios.

Durante:
- Ubicar y activar la zona Triaje “zona de clasificación para la atención de lesionados”.
- Atender al personal lesionado mientras llega la asistencia médica.
- Coordinar acciones para el traslado de personal que requiere atención médica.
- Contabilizar y controlar al personal lesionado.

Después:
- Permanecer en el puesto de primeros auxilios.

- Elaborar un informe de las acciones realizadas durante la emergencia (número de personas atendidas, tipo de lesiones, y los datos del personal trasladado al centro médico).
- Enlistar los materiales utilizados y sustituirlos a la brevedad.
- Entregar el informe a la OSDN.

Brigada de Evacuación

Antes:

- Recibir capacitación de la brigada correspondiente por personas especialistas.
- Observar todo lo que considere un peligro y dar solución a corto, mediano y largo plazo dentro y fuera de las instalaciones.
- Delimitar zonas seguras en cada uno de los pisos.
- Detectar controles eléctricos y determinar quién los va a operar en caso de emergencia.
- Verificar en forma permanentemente los cristales de las ventanas, lámparas, ventiladores, armarios y objetos colgantes que pudieran presentar riesgo.
- Programar recorridos permanentes en el inmueble con la finalidad de observar que las rutas de evacuación se encuentren libres de cualquier obstáculo.
- Instalar las señales y avisos para la protección civil de acuerdo a la norma vigente.

Durante:

- Alejar a la población del área en riesgo.
- Coordinar en la evacuación con las demás brigadas.
- Conducir al personal por la ruta de evacuación previamente establecida a una zona de seguridad.
- Revisar que no quede nadie en el inmueble en caso de desalojo total.
- Mantener el orden del personal durante el desalojo.
- Organizar y controlar al personal en la zona de seguridad interna y externa.
- Pasar lista de conteo en la zona de seguridad interna y externa si así fuera el caso.
- Anotar las ausencias identificadas e informar inmediatamente a la OSDN.
- Permanecer atentos ante cualquier indicación.

Después:

- Participar en la evaluación de la emergencia con el resto de las brigadas.
- Entregar el informe completo a la OSDN.

Brigada Contra Incendios

Antes:

- Conocer el tipo de riesgo al que se enfrentan.
- Recibir capacitación especializada, sobre ataque al fuego.
- Identificar las áreas de mayor riesgo (almacenes).
- Capacitar periódicamente en técnica contra incendios.
- Realizar recorridos permanentes para revisar que los equipos contra incendio portátil y estacionario estén debidamente colocados y listos para usarse en caso de una emergencia, supervisar el buen funcionamiento de equipos (extintores, detectores de humo, hidrantes, etc.)

Durante:

- Al encontrarse cerca del área tomar los extintores más cercanos, accionar los extintores y combatir el conato de incendio.
- Sofocado el conato, colocar a los extintores de manera horizontal sobre el piso (vacíos).
- Antes de retirarse, realizar una revisión visual rápida de las condiciones en que queda el área siniestrada, alejándose de ella.
- En caso de que el fuego se haya extendido solicitar apoyo del exterior

- Coordinar con las otras brigadas para la ayuda a los lesionados.
- Coordinar con la brigada de comunicación para el apoyo de bomberos si la situación lo amerita.

Después:

- De ser necesario ingresar al área de riesgo para realizar una evaluación de las condiciones de seguridad.
- Cerciorarse de que el fuego haya quedado totalmente sofocado.
- Realizar la remoción de escombros.
- Levantar un inventario de los daños materiales.
- Contabilizar el número de extintores utilizados.
- Elaborar un informe sobre el equipo utilizado en el conato de incendio
- Apoyar a las otras brigadas en la elaboración del informe sobre los daños al edificio.
- Entregar el informe a la OSDN.

COMPONENTES DE LAS BRIGADAS DE LA ONPE (*)

SEDE CENTRAL

FUNCIÓN COMO BRIGADISTA	APELLIDOS Y NOMBRES
Jefe de la Brigada	Valenzuela Marroquin Manuel
Brigadista de seguridad	Carrillo Calenzani Oscar Orellana Palomino Carlos
Brigadista de Comunicación	Mori Tafur Aitor Heredia Flores Juan Boluarte García Beatriz
Brigadista de Primeros Auxilios	García Rodriguez Herminio Chero Sipan Joseph Vásquez Ruiz Edwin Razuri Mariñas Percy Zevallos Court Angelo Salinas Gamboa María
Brigadista de Búsqueda y Rescate	Canales Bustamante Reno Martínez Espinoza Edgar Basauri Becerra Marco Rosales Cabanillas Daniel Santos Gutierrez Juan Cajavilca Villarroel Denis Paz Retuerto Frank Calderón Zúñiga Erick
Brigadista de Evacuación	Peralta De la Cruz Carmen Alvizuri Peralta Rafael Figueroa Gallo Edith Schenone Fajardo Graciela Martínez Borja Jhony Polo Bazán Victor Rivera Calderón Jimy Dominguez Jaramillo Felix

	Ayala Richter Fernando Garamendi Campos Jorge Navarro Castellanos Carlos
Brigadista de lucha contra incendio	Gutierrez Coral Luis Vargas Mamani William Romero Santa Cruz Jorge Levano Guillen Alejandro Olortegui Vaquerizo Ruly Alvino López Alcides Condori Soncco José Neyra Zegarra Percy

SEDE CEPSA 1

William Garcia Velasquez
Saúl Salazar Paredes
Oscar Ojeda Rivera
Angelo Luis Morales Díaz
Cesar Silva Burgos

SEDE CEPSA 2

Juan Victorio Montoya
Jorge Reyes Meza
Braulio Pardo Roja

SEDE INDUSTRIAL

Juan Abanto Leiva
Carlos Valer Ramos
Dora Estrella Carbajal

SEDE ANTARES

Román Rivas Camargo
Ivan Pastor Sotomayor
Sara Febres Garcia
Carmen Guevara Regalado

SEDE TALARA

Giuseppe Buitron Grassa
C. Sandoval Cardozo
Christian Flores de la Cruz

(*) Cada sede de la ONPE a nivel nacional, debe llenar este cuadro, de acuerdo a su realidad.

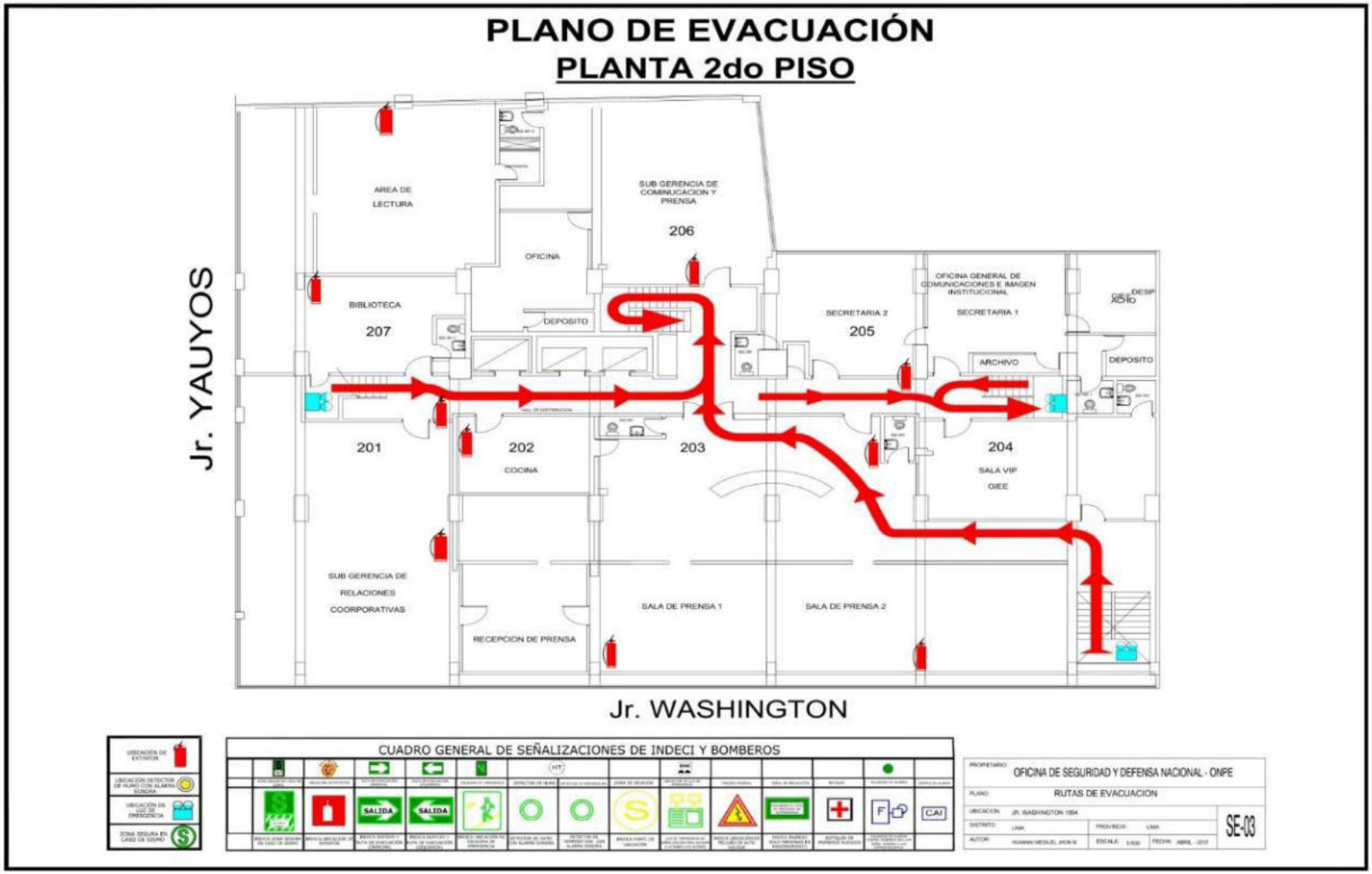
ANEXO D

PLANOS DE EVACUACIÓN DE LAS SEDES (*)

SEDE WASHINGTON

OFICINA DE SEGURIDAD Y DEFENSA NACIONAL

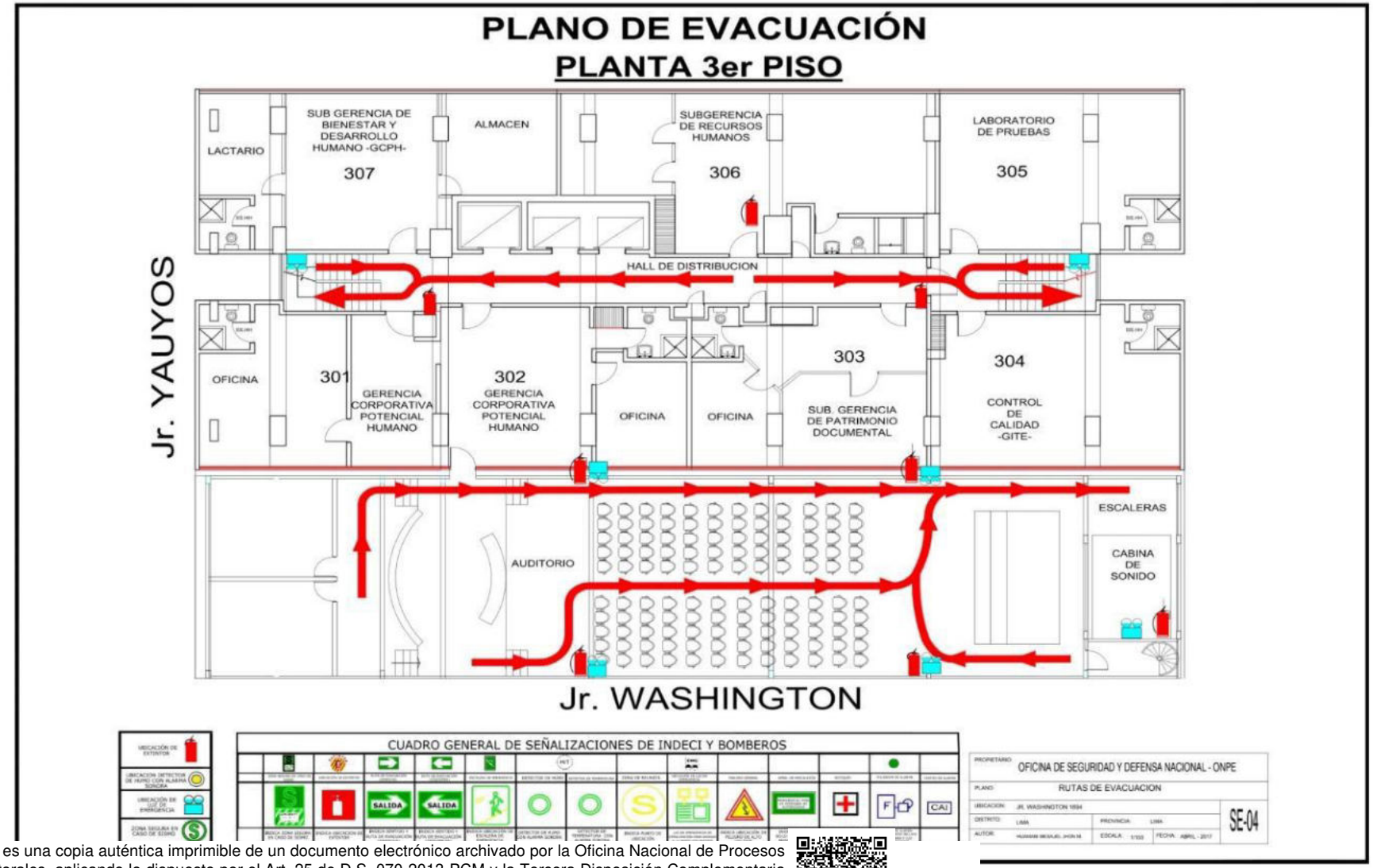
PLANO DE EVACUACIÓN
PLANTA 2do PISO



OFICINA DE SEGURIDAD Y DEFENSA NACIONAL

PLANO DE EVACUACIÓN

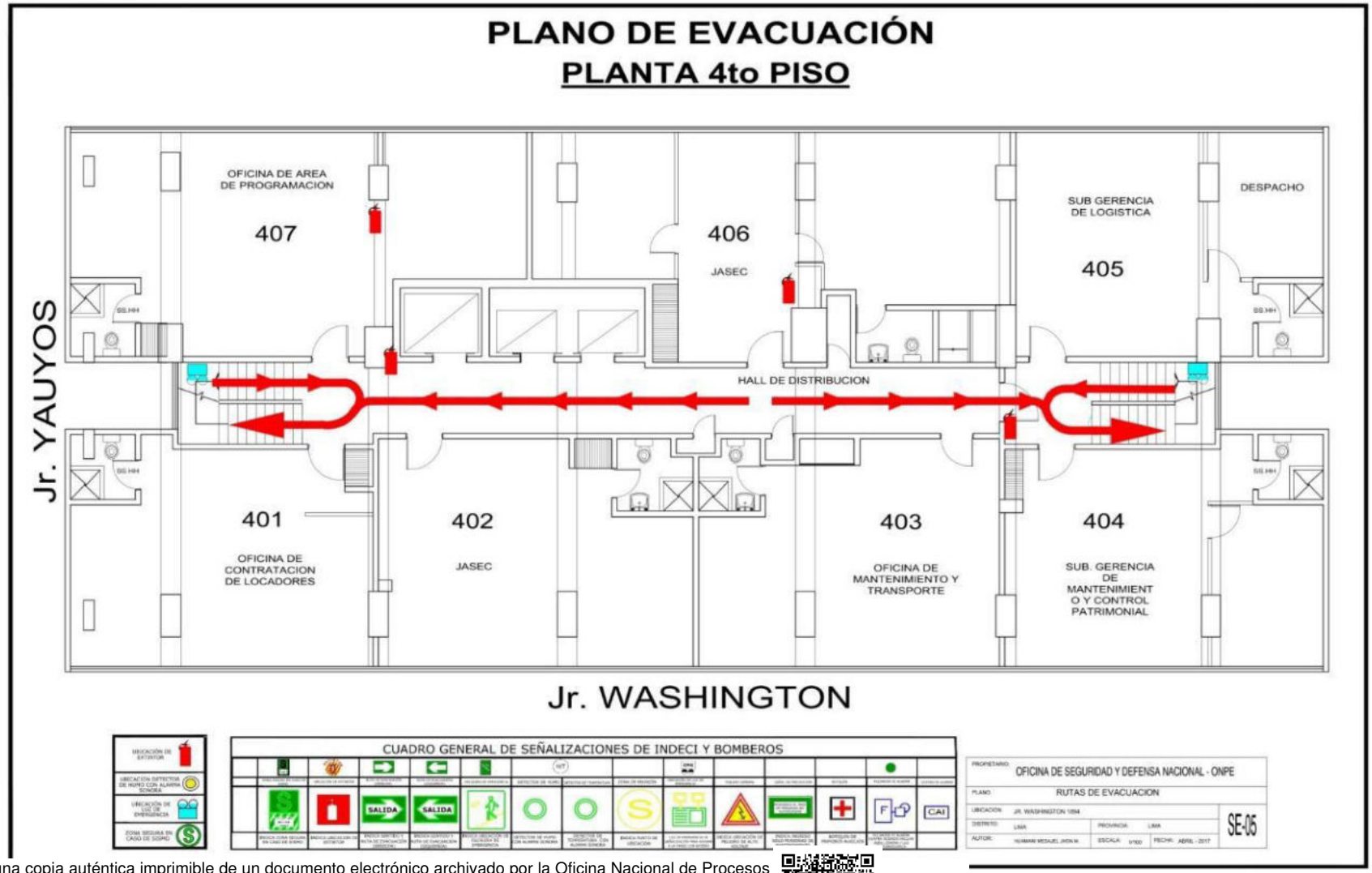
PLANTA 3er PISO



OFICINA DE SEGURIDAD Y DEFENSA NACIONAL

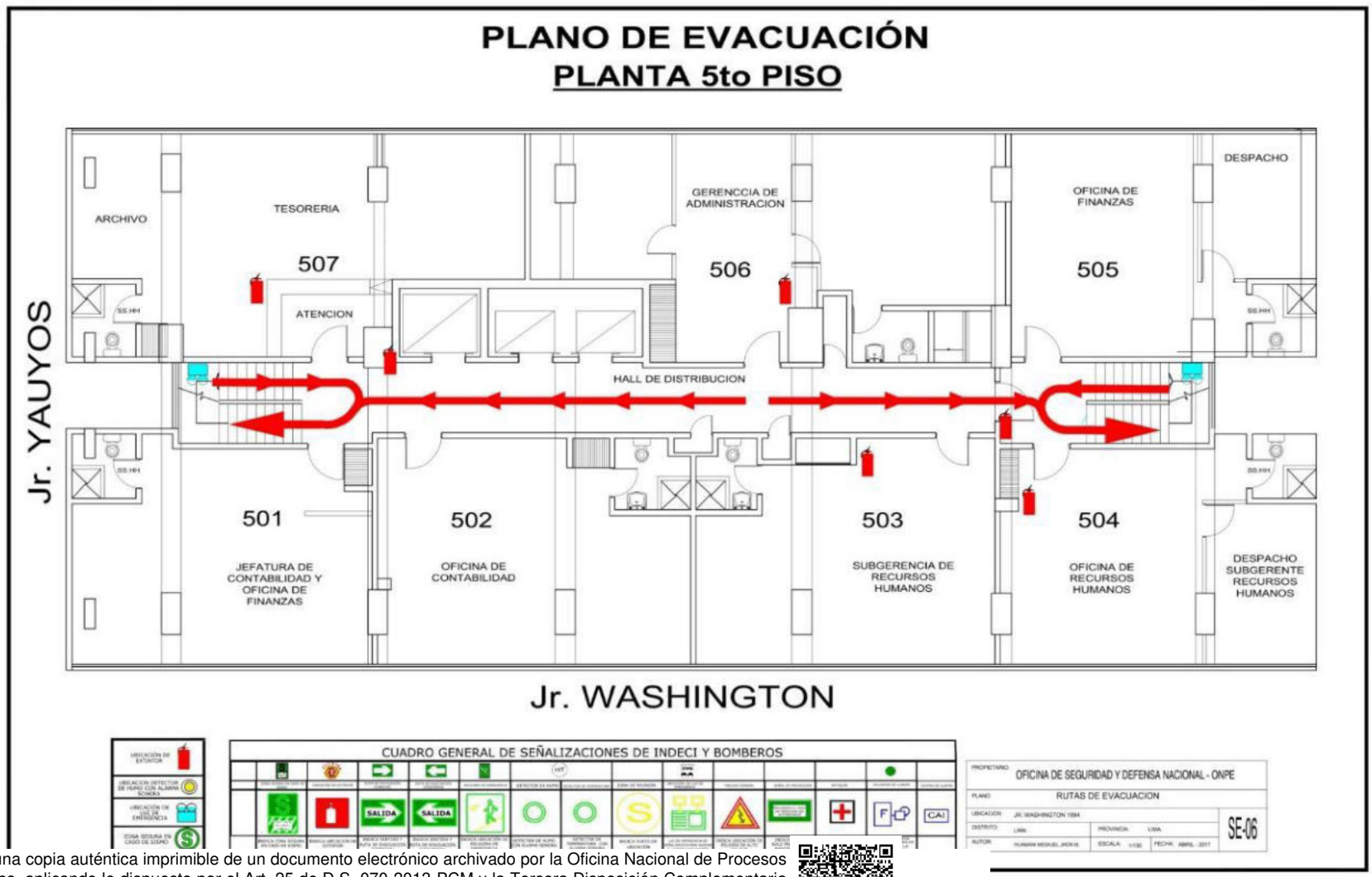
PLANO DE EVACUACIÓN

PLANTA 4to PISO



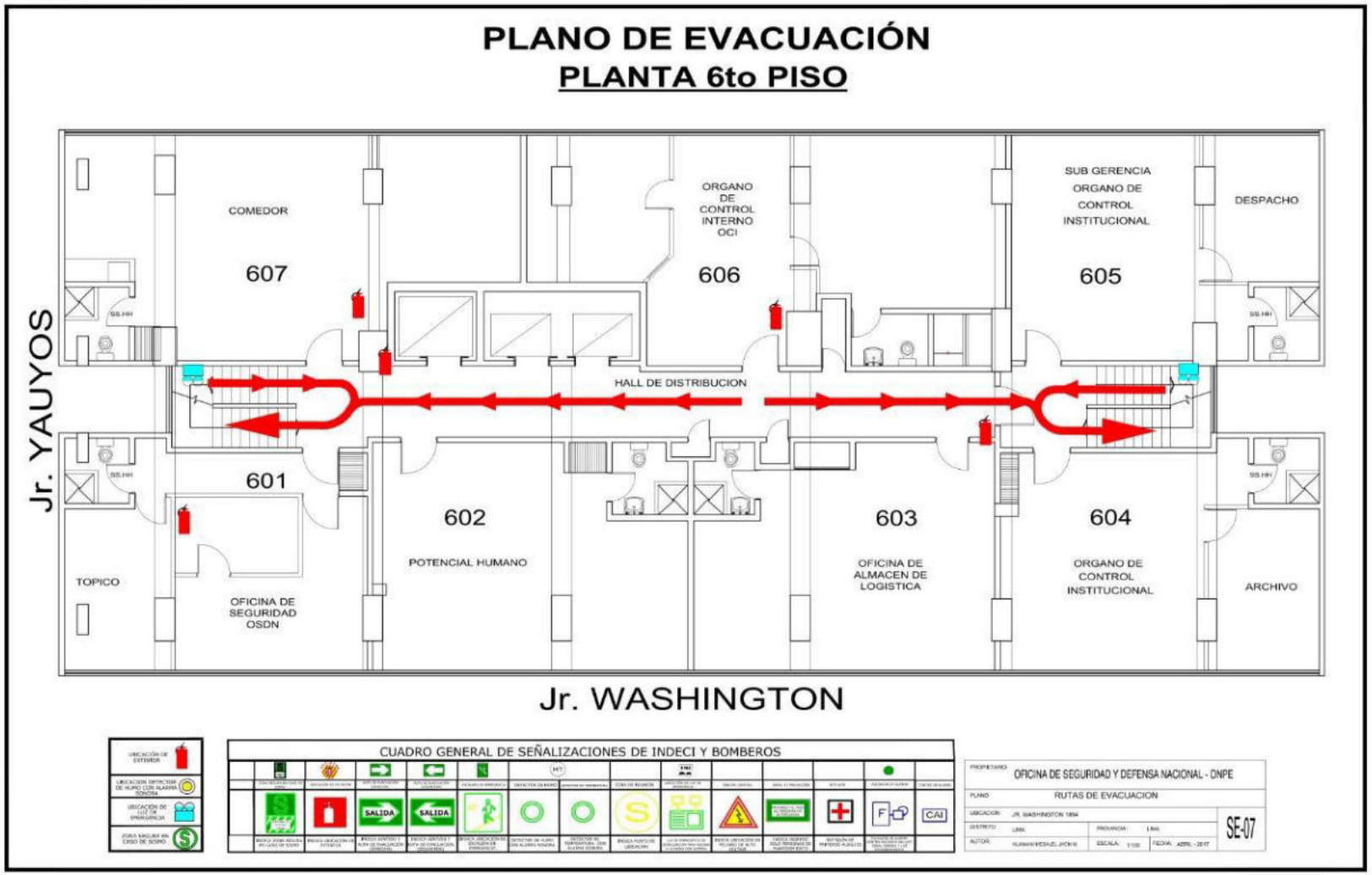
OFICINA DE SEGURIDAD Y DEFENSA NACIONAL

PLANO DE EVACUACIÓN
PLANTA 5to PISO



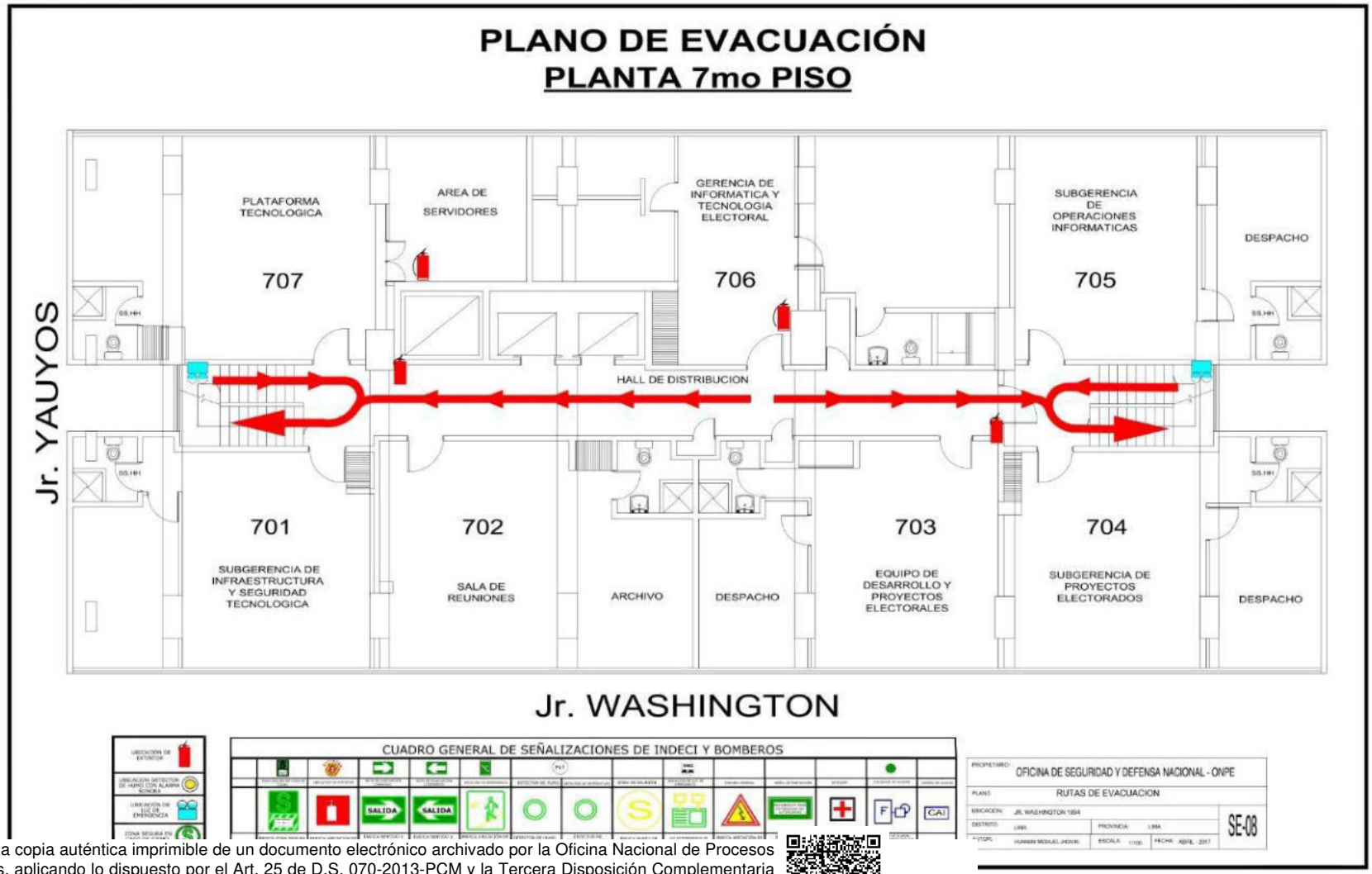
OFICINA DE SEGURIDAD Y DEFENSA NACIONAL

PLANO DE EVACUACIÓN
PLANTA 6to PISO



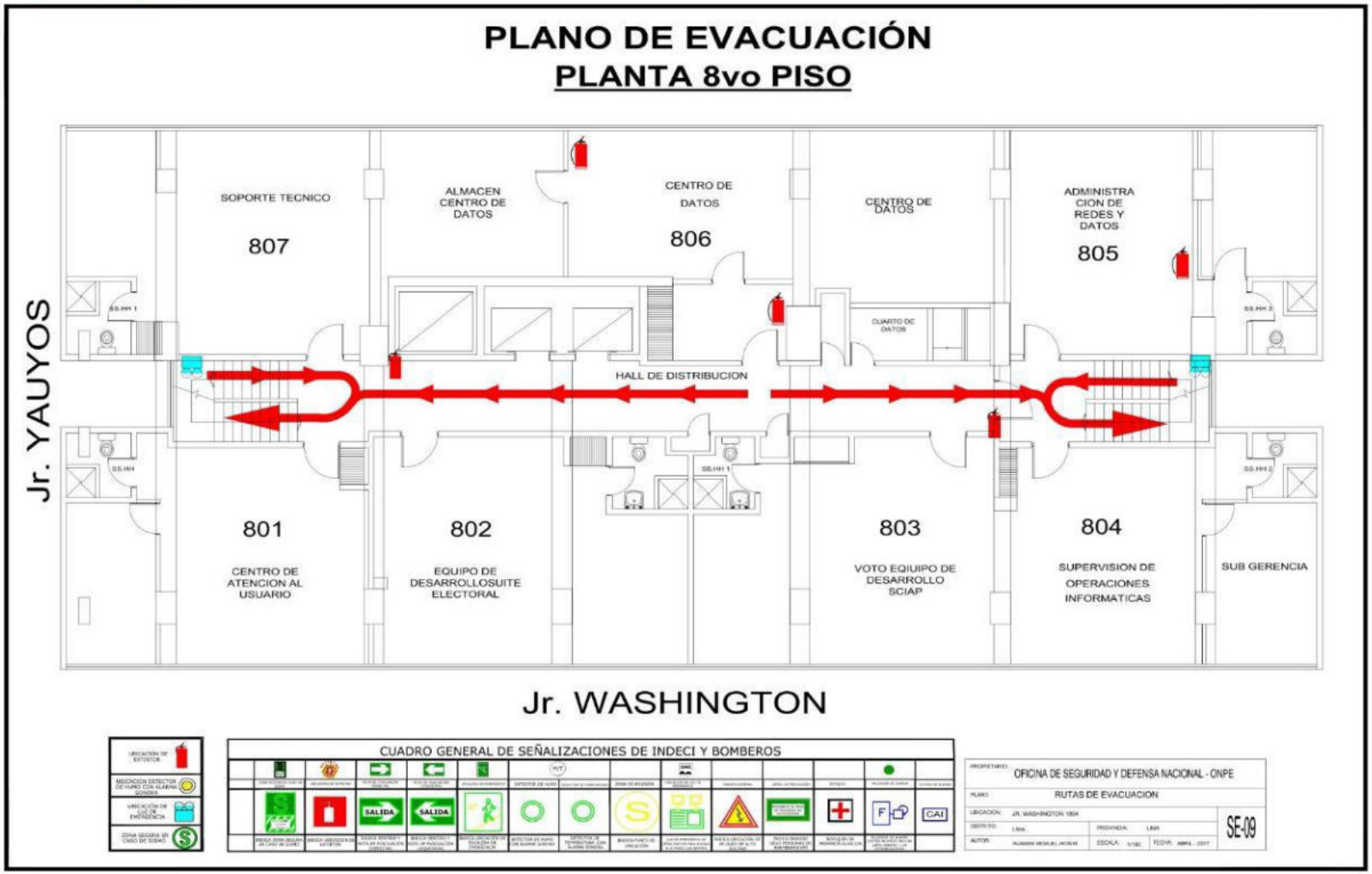
OFICINA DE SEGURIDAD Y DEFENSA NACIONAL

PLANO DE EVACUACIÓN
PLANTA 7mo PISO

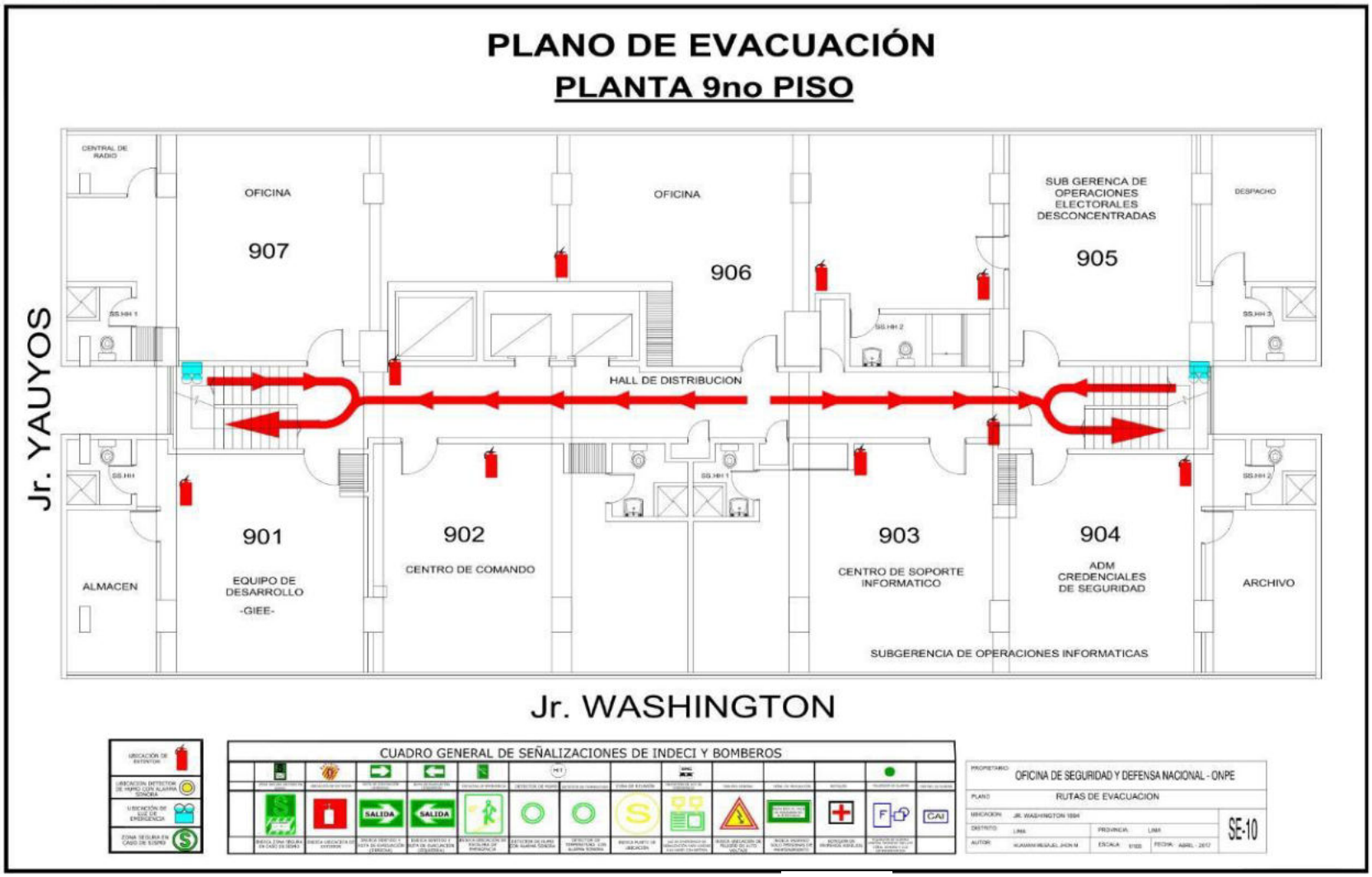


OFICINA DE SEGURIDAD Y DEFENSA NACIONAL

PLANO DE EVACUACIÓN
PLANTA 8vo PISO



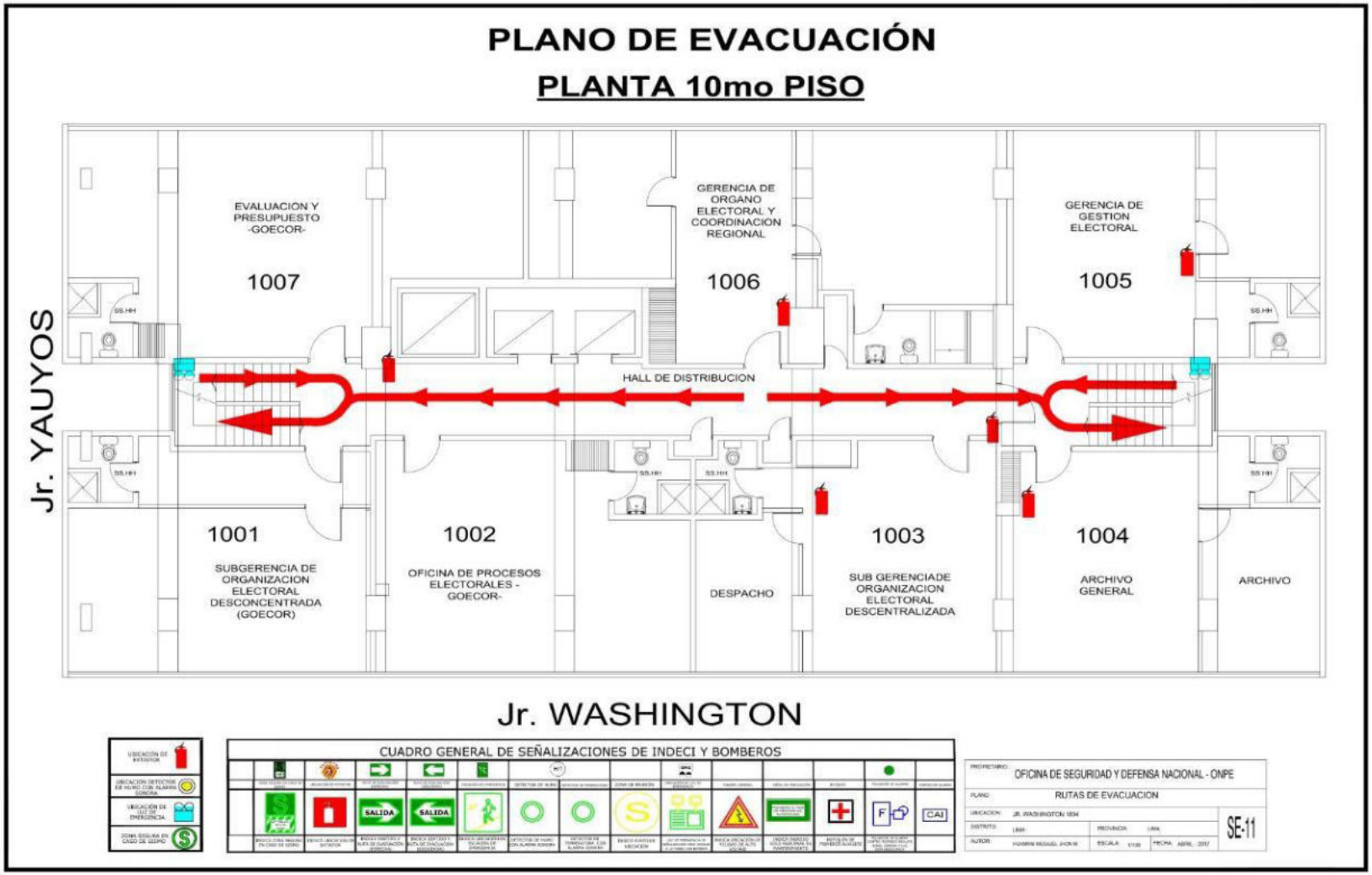
OFICINA DE SEGURIDAD Y DEFENSA NACIONAL



OFICINA DE SEGURIDAD Y DEFENSA NACIONAL

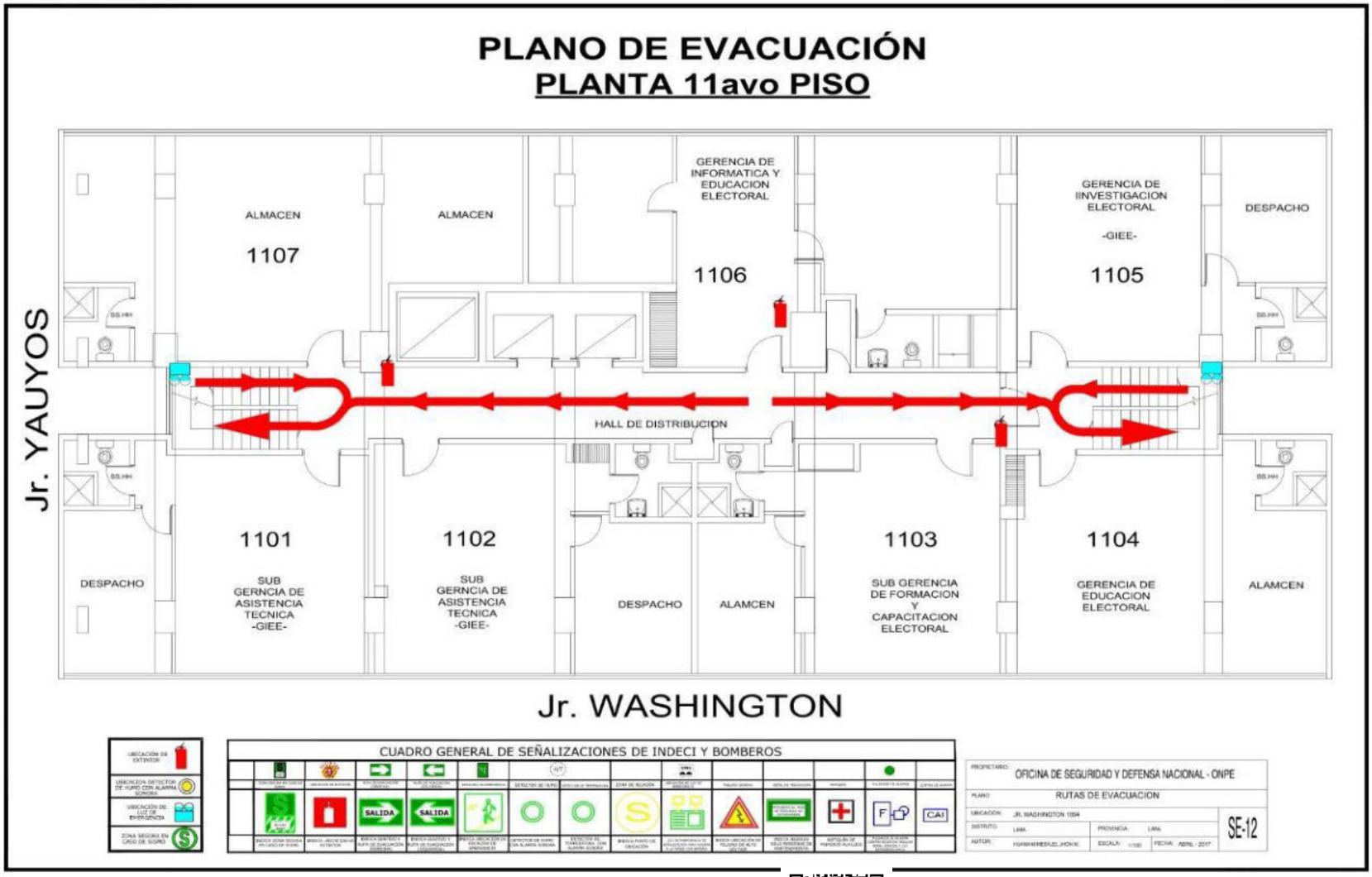
PLANO DE EVACUACIÓN

PLANTA 10mo PISO



OFICINA DE SEGURIDAD Y DEFENSA NACIONAL

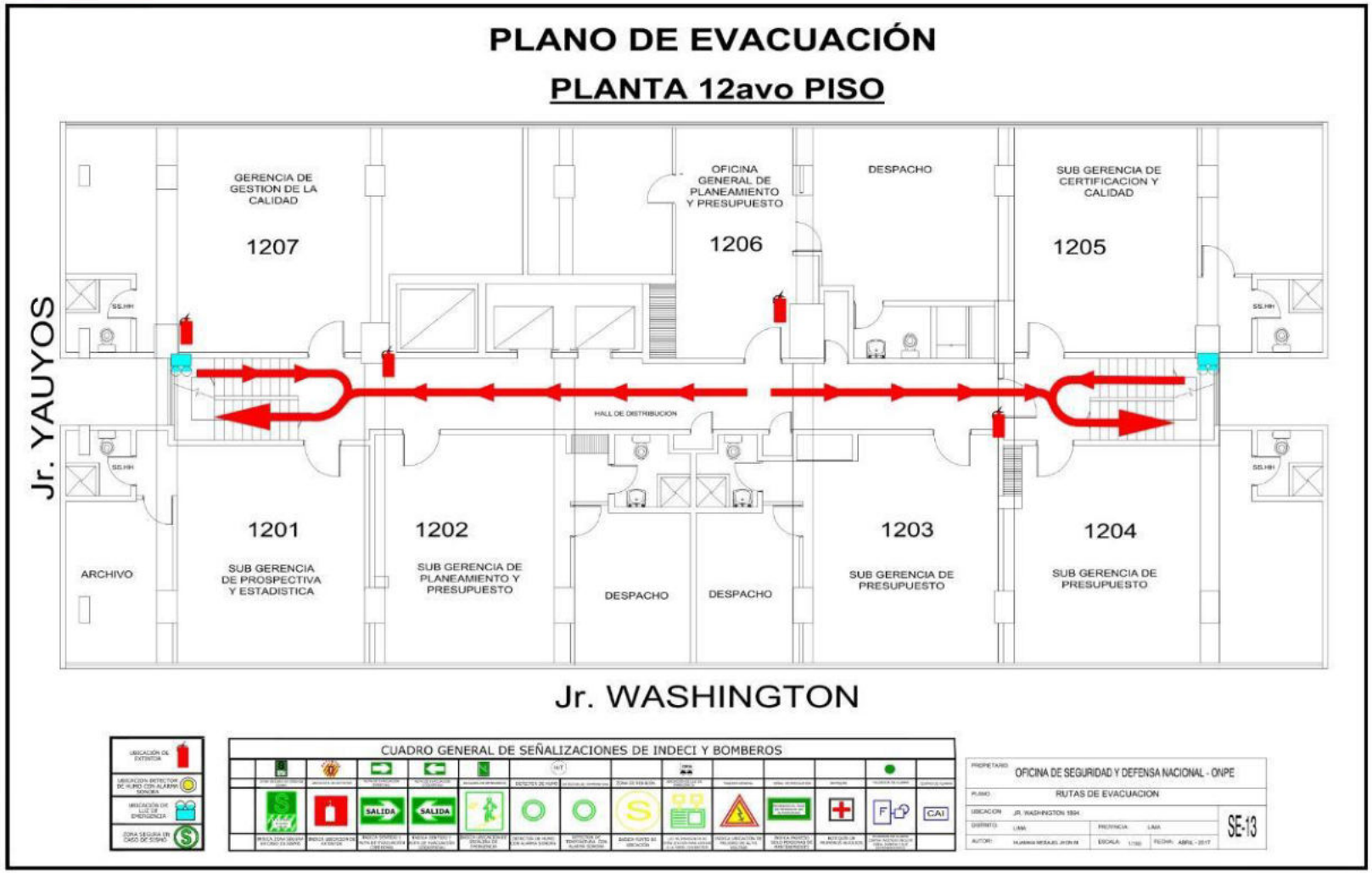
PLANO DE EVACUACIÓN
PLANTA 11avo PISO



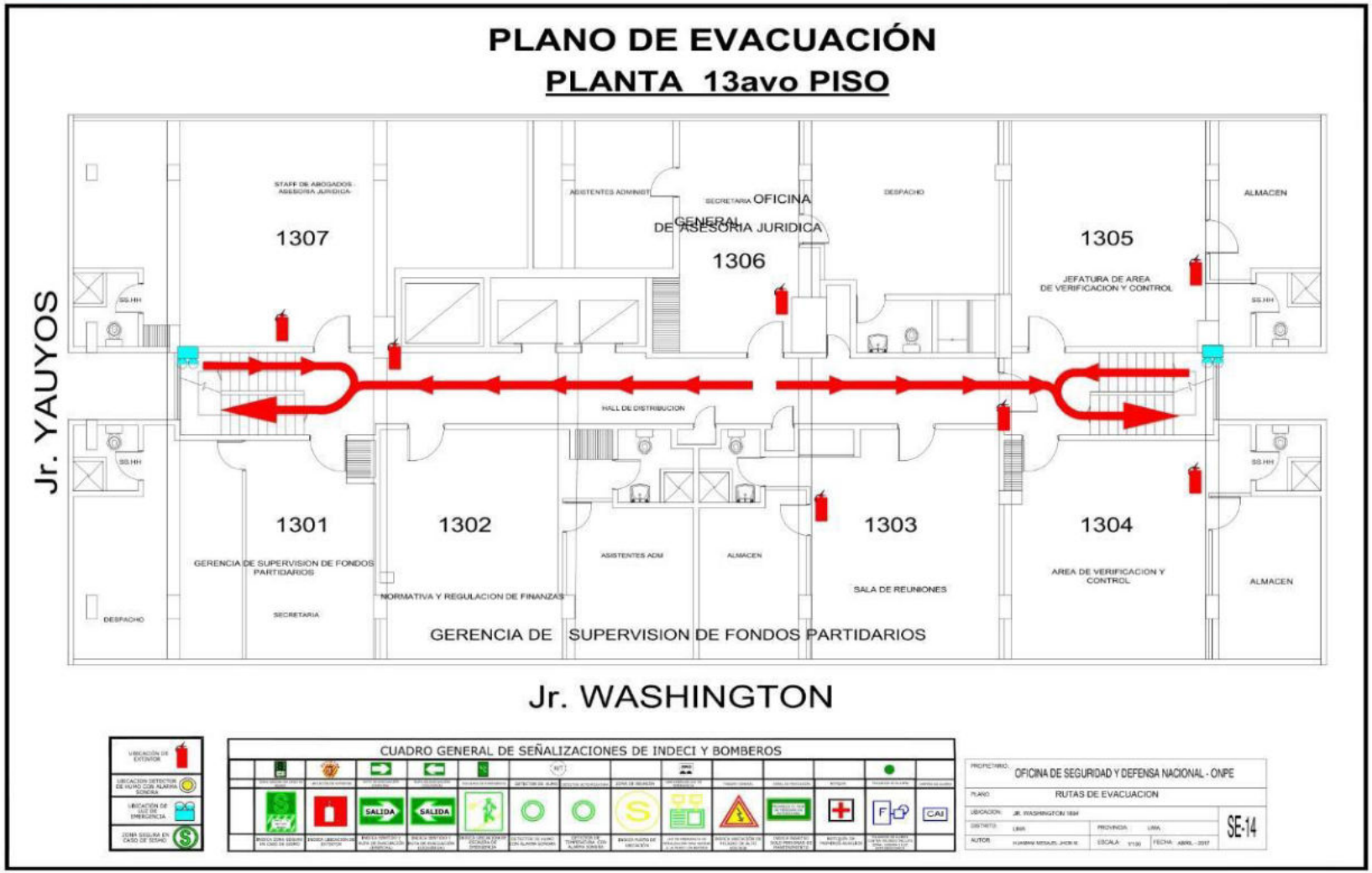
OFICINA DE SEGURIDAD Y DEFENSA NACIONAL

PLANO DE EVACUACIÓN

PLANTA 12avo PISO



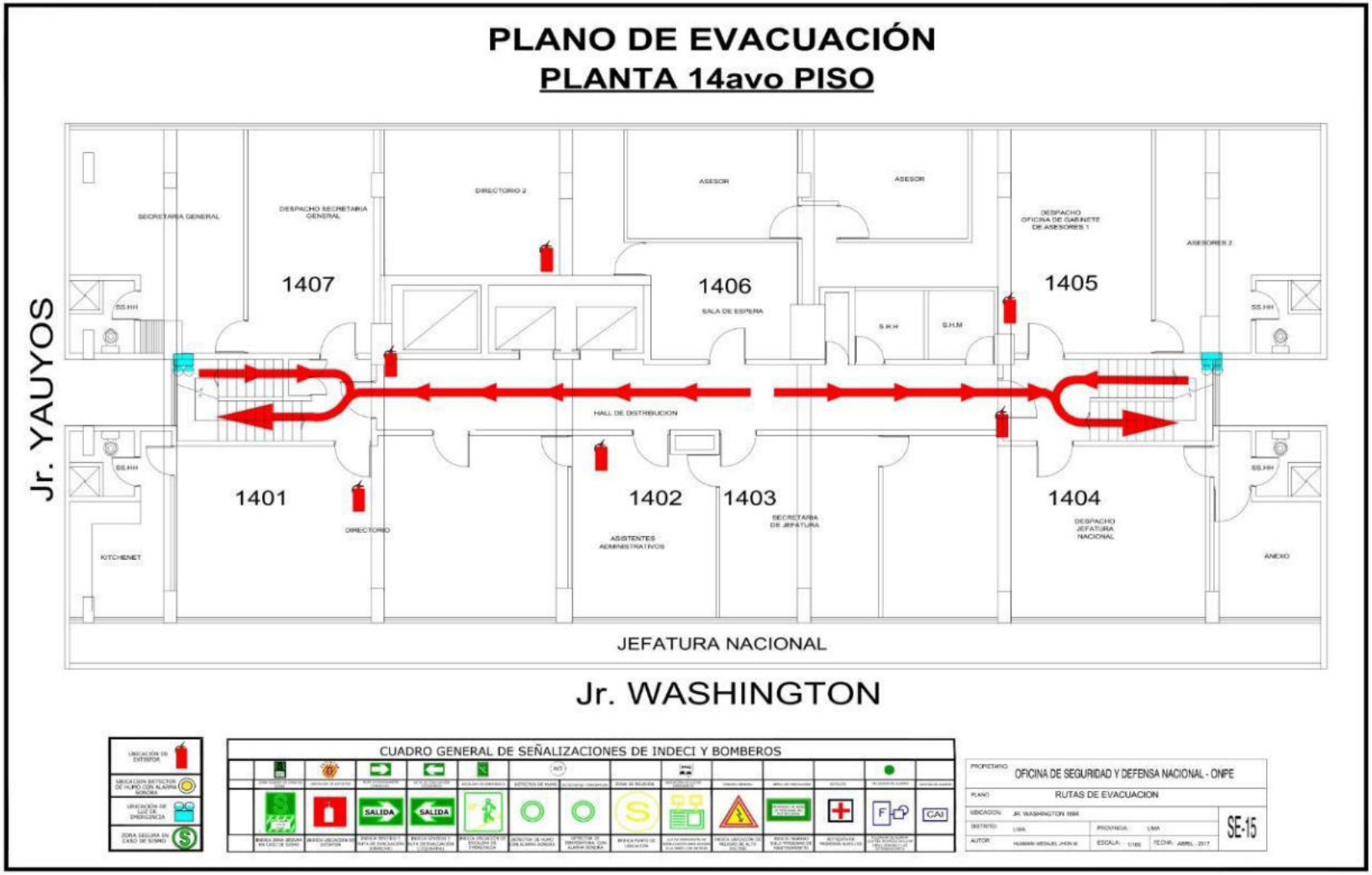
OFICINA DE SEGURIDAD Y DEFENSA NACIONAL



OFICINA DE SEGURIDAD Y DEFENSA NACIONAL

PLANO DE EVACUACIÓN

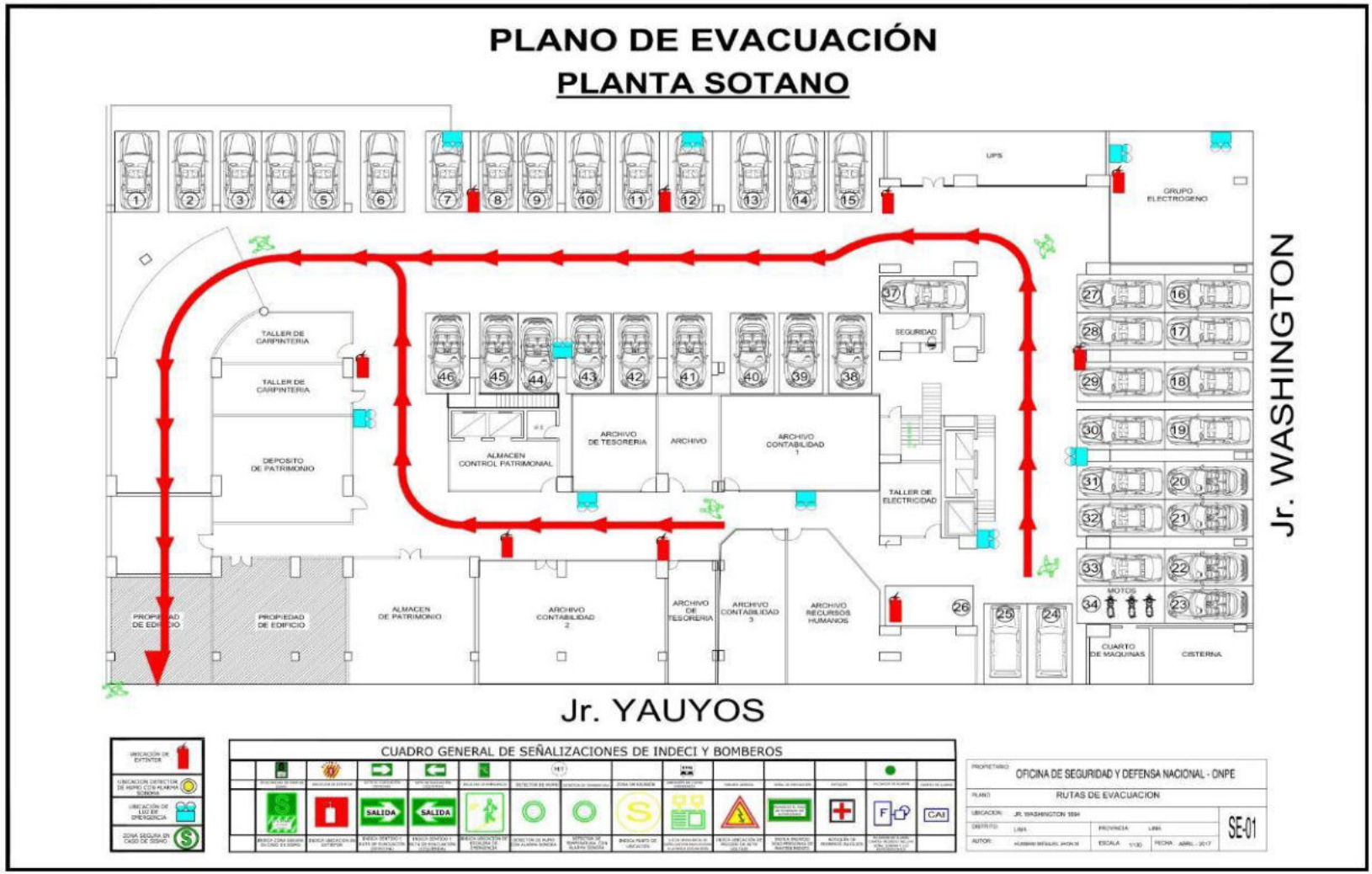
PLANTA 14avo PISO



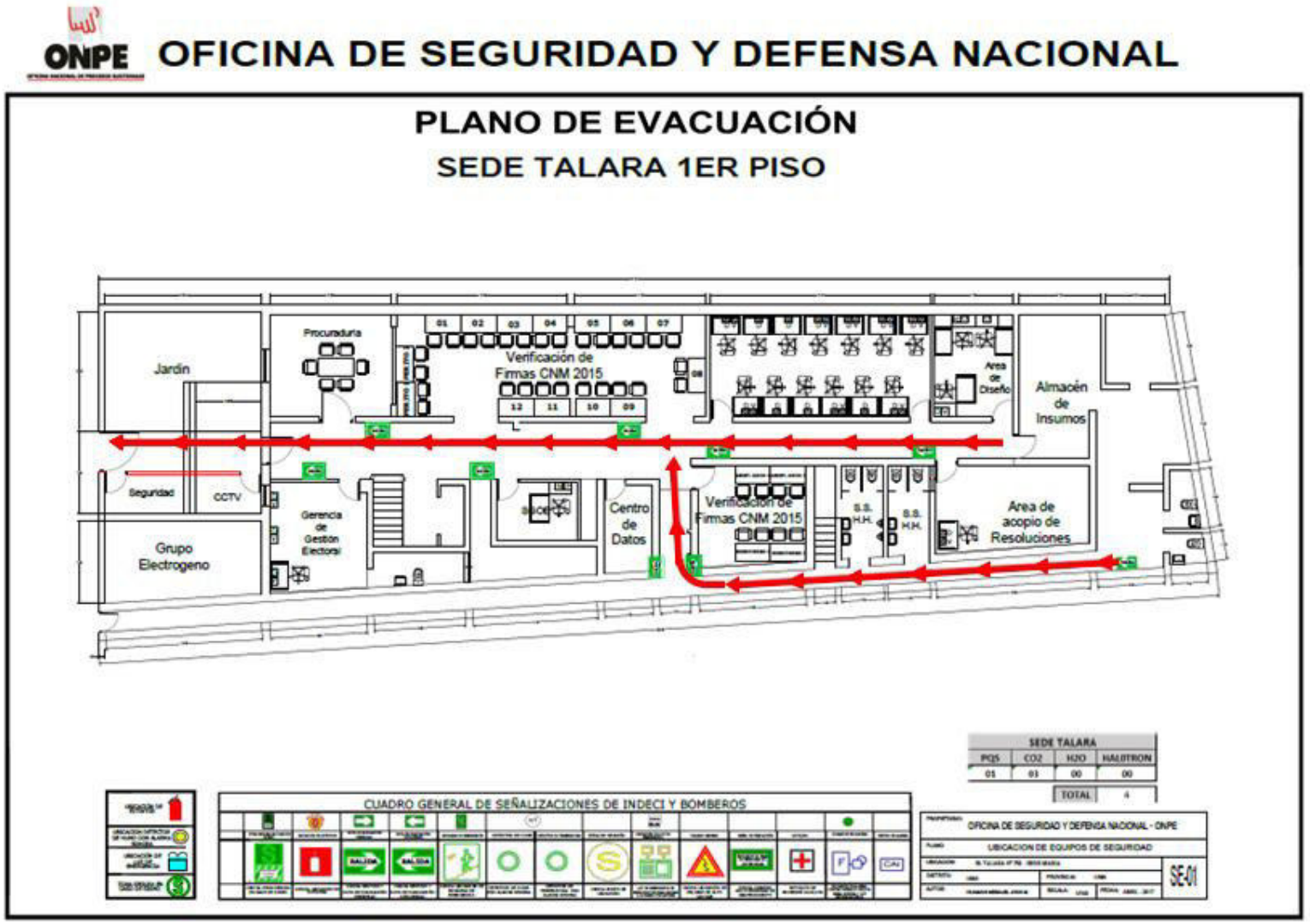
OFICINA DE SEGURIDAD Y DEFENSA NACIONAL

PLANO DE EVACUACIÓN

PLANTA SOTANO



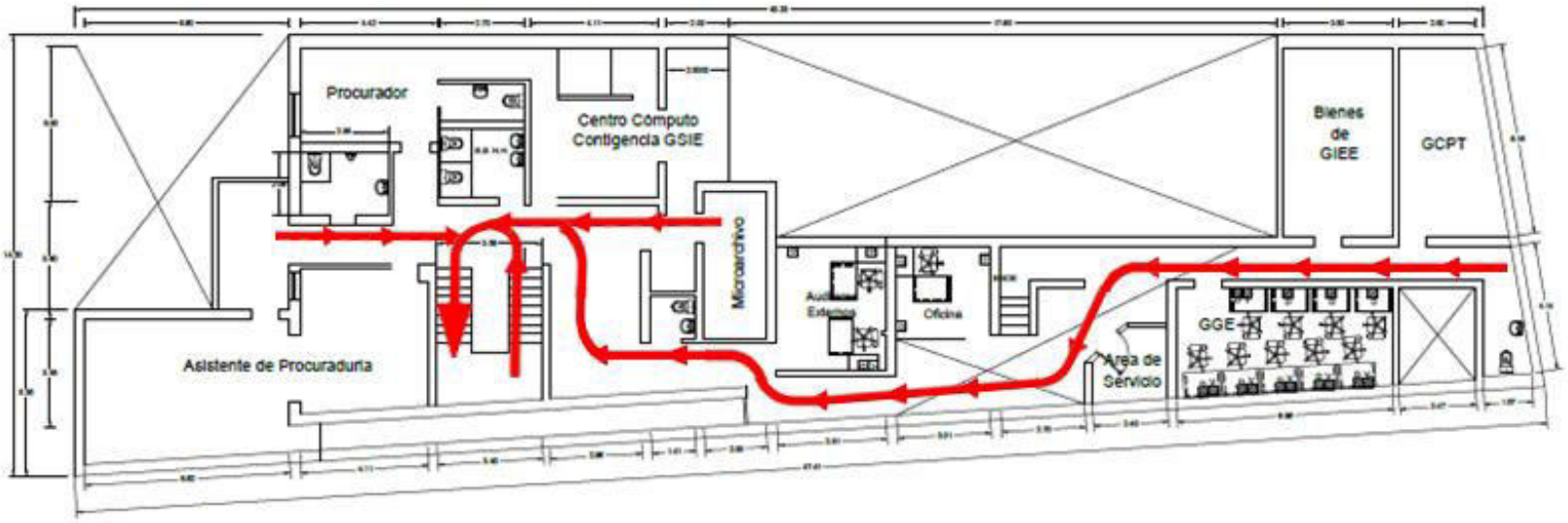
SEDE TALARA



OFICINA DE SEGURIDAD Y DEFENSA NACIONAL

PLANO DE EVACUACIÓN

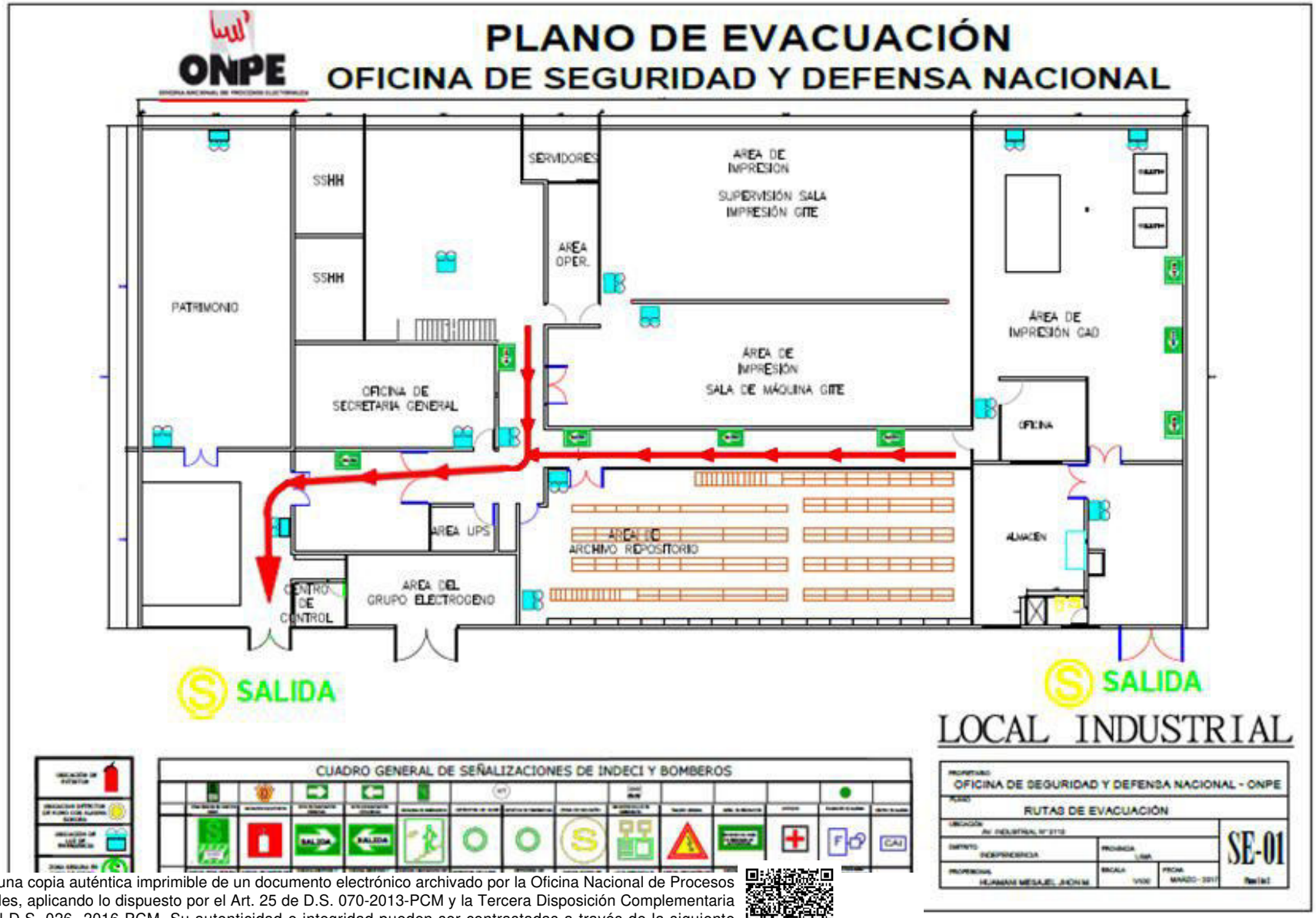
SEDE TALARA 2DO PISO



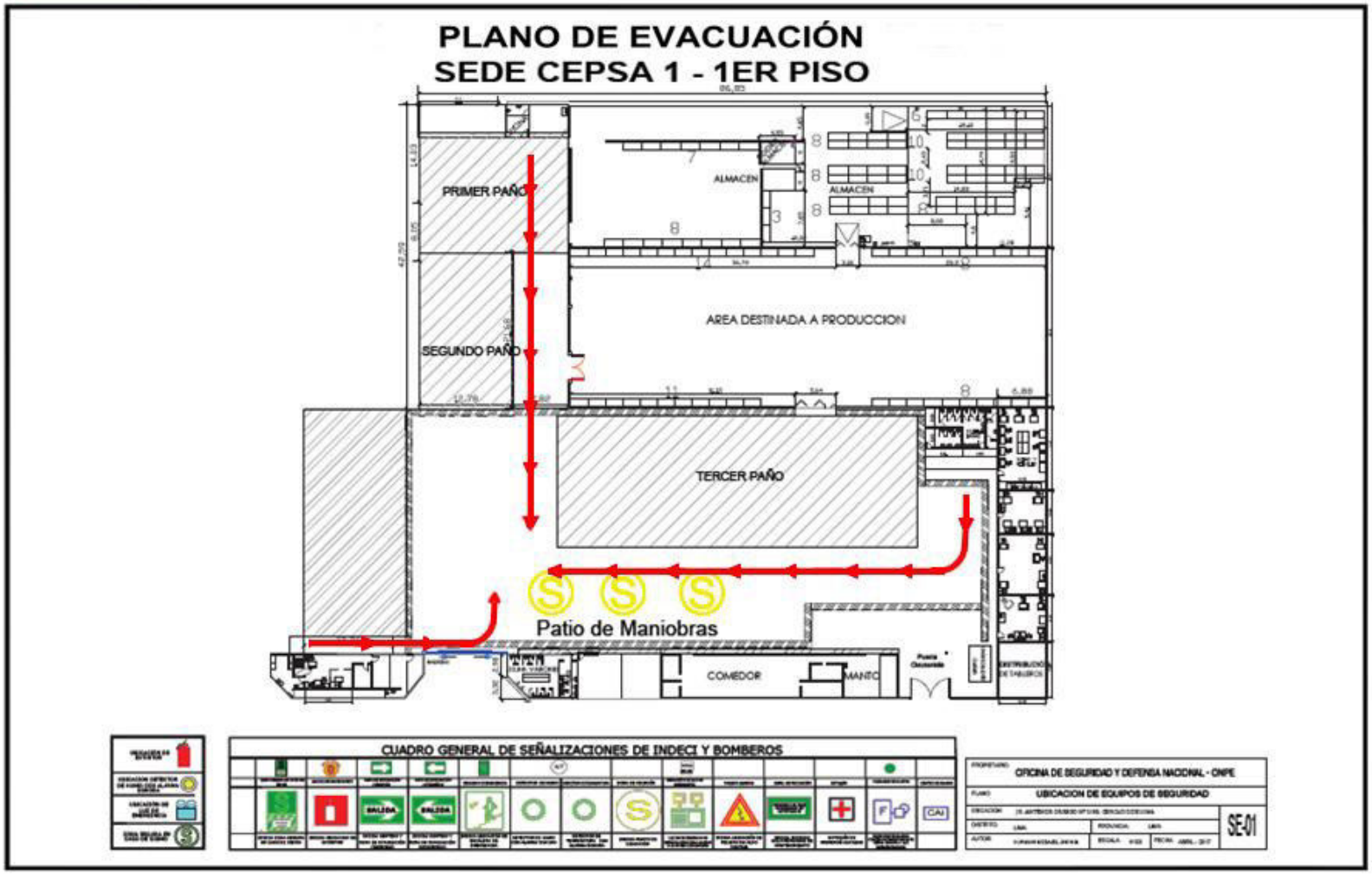
SEDE TALARA			
PQS	CO2	H2O	HALOTRON
00	04	00	00
TOTAL	4		

PROPIETARIO:	OFICINA DE SEGURIDAD Y DEFENSA NACIONAL - ONPE
PLANO:	UBICACION DE EQUIPOS DE SEGURIDAD
UBICACION:	
DISTRITO:	PROVINCIA: REGION:
AUTOR:	FECHA:

SE-02

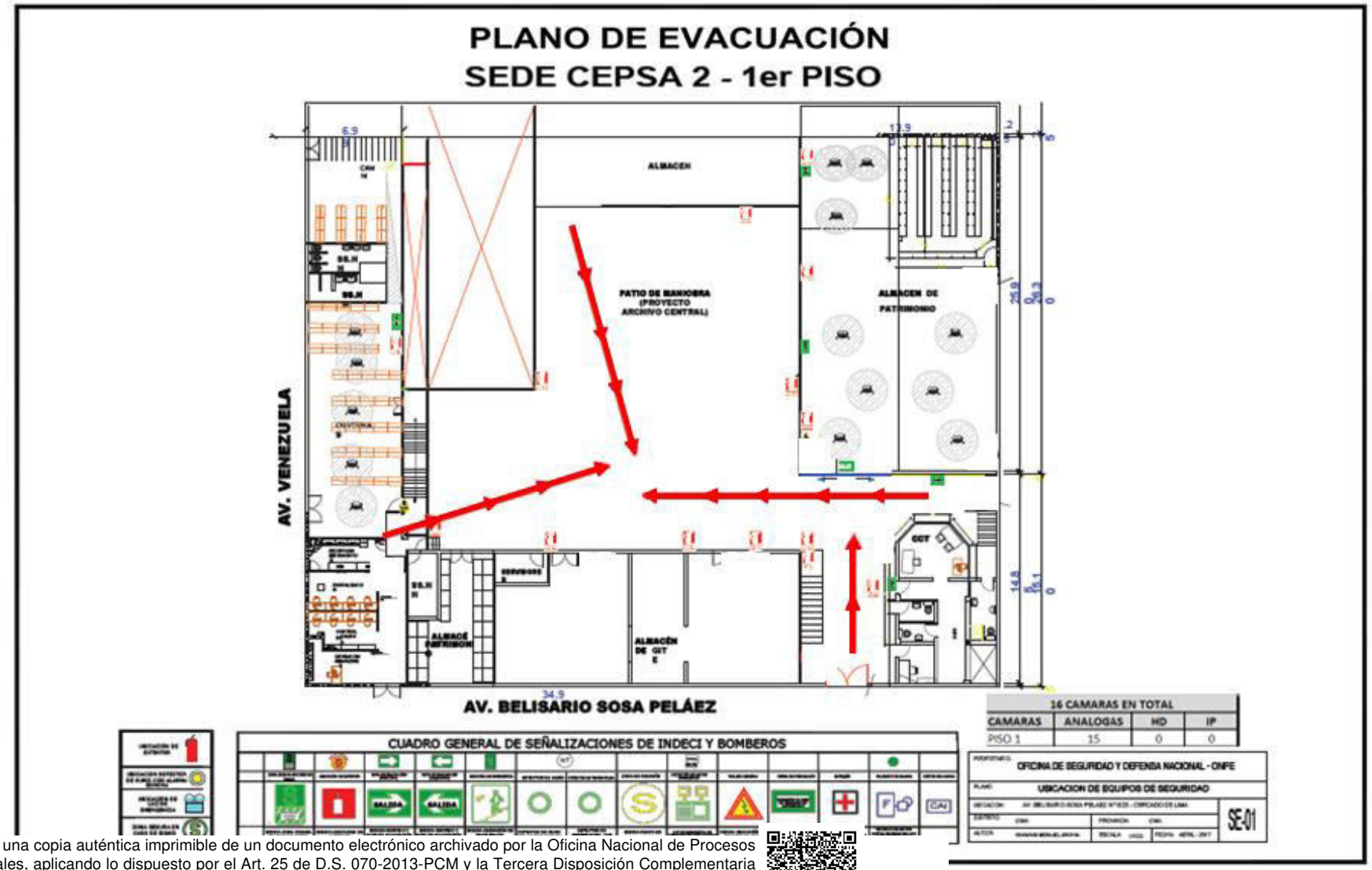


OFICINA DE SEGURIDAD Y DEFENSA NACIONAL

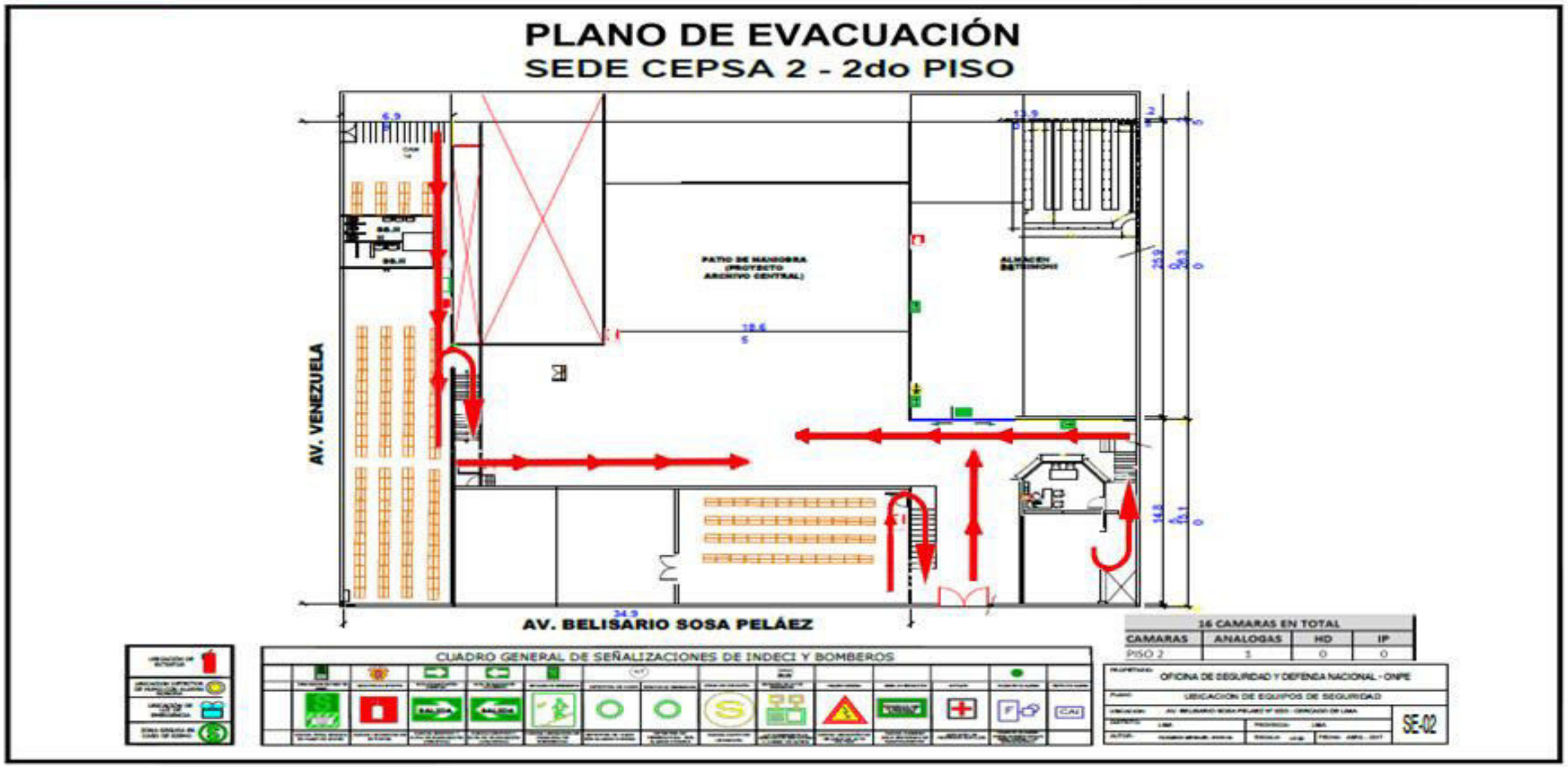


OFICINA DE SEGURIDAD Y DEFENSA NACIONAL

PLANO DE EVACUACIÓN
SEDE CEPSA 2 - 1er PISO



SEDE CEPSA 2



(*) Cada sede de la ONPE a nivel nacional, debe elaborar sus planos, de acuerdo a su realidad.

ANEXO E

INFORMACIÓN SOBRE LAS SEDES DE LA ONPE (*)

SEDE CENTRAL

A. Ubicación geográfica: (Av., Jr., Calle, N°, 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: La sede central monitorea las 60 ODPE previstas para las ECE 2020.

D. Información relevante:

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

LOCALIDAD	NOMBRE DEL CENTRO DE ATENCIÓN MEDICA	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 - 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 Roma 2.	Jr. Junín 568
Cercado – Lima	Cía. Bomberos France 3	Jr. Moquegua 240

(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 – Lima	Comisaria Petit Thouars	Av. Petit Thouars 455.

- No existe antecedentes 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.

(4) Partidos Políticos:

LOCALIDAD	NOMBRE DEL PARTIDO POLÍTICO	DIRECCIÓN
Cercado - Lima	Acción Popular	Av. Paseo Colon 422
Cercado - Lima	Fuerza Popular	Av. Paseo Colon 260
Breña	PPC	Av. Alfonso Ugarte 1484

E. Actividades de seguridad previstas

N°	ACTIVIDAD	PROGRAMACIÓN								
		FECHA		META ANUAL	UNIDAD DE MEDIDA					
		INICIO	TERMINO			OCT	NOV	DIC	ENE	FEB
1	Emisión de Oficios solicitando al CCFFAA y PNP designación de Oficiales Enlace y/o Coordinadores	01/10/2019	31/10/2019	1		1				
2	Emisión de Oficios solicitando custodia Policial para las sede de la ODPE	01/12/2019	30/12/2019	1				1		
3	Emisión de oficios solicitando resguardo policial para el desplazamiento del material electoral	01/10/2019	28/02/2020	5		1	1	1	1	1
4	Coordinación de Seguridad con las FFAA y PNP	01/11/2019	31/01/2020	3			1	1	1	
5	Entrega de cartilla de seguridad para las FFAA y PNP	01/11/2019	30/12/2019	1				1		
6	Entrega de cartilla informativa para el MP	01/11/2019	30/12/2019	1				1		

F. Características de las Instalaciones:

SEDE	MATERIAL DE CONSTRUCCIÓN	ESTADO DE CONSERVACIÓN DEL LOCAL	AREA	PISOS	N° DE CUARTOS	AFORO	POSEE ENERGÍA ELÉCTRICA	POSEE AGUA Y DESAGUE	TELÉFONO	INTERNET	GRADO DE SEGURIDAD QUE DISPONE EL LOCAL
CENTRAL	NOBLE	REGULAR	10,227.6 M2	14+ SÓTANO Y AZOTEA	98	800	SI	SI	SI	SI	BUENA

(*) Cada sede de la ONPE a nivel nacional, debe completar esta información, de acuerdo a su realidad.

Anexo "F" PR01-OSDN/SP Seguridad del Proceso Electoral

ONPE	PROCEDIMIENTO	Código:	PR01-OSDN/SP
		Versión:	02
	SEGURIDAD DEL PROCESO ELECTORAL	Página:	1 de 21

Elaborado por:	Revisado por:	Aprobado por:
Luis Enrique Sifuentes Leonardo Especialista en Seguridad y Defensa Nacional 08 AGO 2016	Fernando López Villafuerte Gerente de la Oficina de Seguridad y Defensa Nacional 15 AGO 2016 Jaime Enrique Moline Vilchez Gerente de Gestión de la Calidad 15 AGO 2016	Fernando López Villafuerte Gerente de la Oficina de Seguridad y Defensa Nacional 15 AGO 2016

1. OBJETIVO:

Establecer las actividades para realizar la secuencia de medidas preventivas en materia de seguridad con el propósito de garantizar el normal desarrollo de los procesos electorales, referéndum y consultas populares organizados por la ONPE.

2. ALCANCE:

Es de aplicación de la Gerencia General, la Oficina de Seguridad y Defensa Nacional, la Gerencia de Gestión Electoral, la Gerencia de Organización Electoral y Coordinación Regional, las Oficinas Descentralizadas de Procesos Electorales y las Oficinas Regionales de Coordinación.

3. BASE NORMATIVA:

3.1. Constitución Política del Perú.
3.2. Ley N° 26859, Ley Orgánica de Elecciones.
3.3. Ley N° 26487, Ley Orgánica de la Oficina Nacional de Procesos Electorales.
3.4. Ley N° 27683, Ley de Elecciones Regionales.
3.5. Ley N° 26864, Ley de Elecciones Municipales.
3.6. Ley N° 28094, Ley de Partidos Políticos.
3.7. Código Penal.
3.8. Ley N° 27408, Ley de Atención Preferente.
3.9. Convocatorias a procesos electorales, consultas populares y referéndums.

Nota: Los documentos mencionados son los vigentes incluyendo sus modificaciones.

4. REFERENCIAS:

4.1. PR01-GGE/DMS Despliegue de material de sufragio y/o equipos informáticos, material de reserva y paquete de coordinador de local de votación a ODPE provincia y LV en Lima Metropolitana y Callao
4.2. PR01-GGE/RME Repliegue de material electoral, equipos informáticos y documentos electorales.

[ ]

Nota: Los documentos mencionados son los vigentes incluyendo sus modificaciones.

5. DEFINICIONES Y ABREVIATURAS:

5.1. Definiciones:

5.1.1. PROVIAS
Proyecto especial del Ministerio de Transportes y Comunicaciones, con autonomía técnica, administrativa y financiera, encargado de realizar proyectos de construcción, mejoramiento, rehabilitación y mantenimiento de la red vial nacional.

5.2. Abreviaturas:

5.2.1. CC.FF.AA.
Comando Conjunto de las Fuerzas Armadas.

5.2.2. FF.AA.
Fuerzas Armadas.

5.2.3. GG
Gerencia General

5.2.4. GGE
Gerencia de Gestión Electoral.

5.2.5. GIEE
Gerencia de Información y Educación Electoral.

5.2.6. GOECOR
Gerencia de Organización Electoral y Coordinación Regional.

5.2.7. GCRC
Gerencia de Comunicaciones y Relaciones Corporativas

5.2.8. GPP
Gerencia de Planeamiento y Presupuesto

5.2.9. INDECI
Instituto Nacional de Defensa Civil.

5.2.10. JEE
Jurado Electoral Especial.

5.2.11. JNE
Jurado Nacional de Elecciones.

5.2.12. MP
Ministerio Público

5.2.13. ODPE
Oficina Descentralizada de Procesos Electorales.

5.2.14. OE
Oficial de enlace.

5.2.15. ORC
Oficina Regional de Coordinación

5.2.16. PNP
Policía Nacional del Perú.

5.2.17. PJFSDJ
Presidentes de las Juntas de Fiscales Superiores de los Distritos Judiciales.

5.2.18. RENIEC
Registro Nacional de Identificación y Estado Civil.

5.2.19. RJ
Resolución Jefatural.

6. RESPONSABLES:

6.1. La Gerencia General GG es la encargada de coordinar con los organismos del sistema electoral.

6.2. La Gerencia de OSDN es responsable de coordinar con las autoridades competentes las acciones destinadas a garantizar la seguridad ciudadana durante los procesos electorales. Así como cumplir y hacer cumplir el presente procedimiento, asegurando su implementación y control respectivo.

6.3. El Gerente de la GOECOR es responsable de hacer cumplir el procedimiento a través de las ODPE y/o ORC.

6.4. El Jefe de la ODPE, el Responsable de la ORC o quien haga sus veces, son responsables de realizar las actividades tal como lo indica este procedimiento.

5.2.12. MP
Ministerio Público

5.2.13. ODPE
Oficina Descentralizada de Procesos Electorales.

5.2.14. OE
Oficial de enlace.

5.2.15. ORC
Oficina Regional de Coordinación

5.2.16. PNP
Policía Nacional del Perú.

5.2.17. PJFSDJ
Presidentes de las Juntas de Fiscales Superiores de los Distritos Judiciales.

5.2.18. RENIEC
Registro Nacional de Identificación y Estado Civil.

5.2.19. RJ
Resolución Jefatural.

6. RESPONSABLES:

6.1. La Gerencia General GG es la encargada de coordinar con los organismos del sistema electoral.

6.2. La Gerencia de OSDN es responsable de coordinar con las autoridades competentes las acciones destinadas a garantizar la seguridad ciudadana durante los procesos electorales. Así como cumplir y hacer cumplir el presente procedimiento, asegurando su implementación y control respectivo.

6.3. El Gerente de la GOECOR es responsable de hacer cumplir el procedimiento a través de las ODPE y/o ORC.

6.4. El Jefe de la ODPE, el Responsable de la ORC o quien haga sus veces, son responsables de realizar las actividades tal como lo indica este procedimiento.

	PROCEDIMIENTO	Código:	PR01-OSDN/SP
ONPE		Versión:	02
	SEGURIDAD DEL PROCESO ELECTORAL	Página:	4 de 21

7. DESARROLLO:

7.1. Elaboración de Disposiciones e instrucciones en materia de seguridad

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
Elaborar proyecto de las Disposiciones para garantizar el orden, la seguridad y la libertad personal durante los procesos electorales. Nota: Se puede tomar como referencia las disposiciones de la última elección de similares características.	Gerente de OSDN o quien delegue	----
Remitir los proyectos de las Disposiciones e instrucciones, la Resolución para su aprobación y el Informe a la Jefatura Nacional. Nota: Realizar correcciones en caso lo solicite la JN.	Gerente de OSDN o quien delegue	Informe
Elaborar oficios para la remisión de las Disposiciones aprobadas a la Secretaría General del Ministerio Público, al Jefe del Comando Conjunto de las Fuerzas Armadas y al Director General de la Policía Nacional del Perú. [ ]	Gerente de OSDN o quien delegue	Oficio

7.2. Solicitud para designación de OE de la PNP y del CC.FF.AA.

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
[ ]	[ ]	[ ]
Emitir oficios dirigidos al Jefe del CC.FF.AA. y al Director General de la PNP, solicitando que se designe a los oficiales de enlaces de sus respectivas Instituciones ante la ONPE. Nota: Adjuntar a los oficios las publicaciones del diario oficial El Peruano, sobre la convocatoria a los procesos electorales.	Gerente de OSDN o quien delegue	Oficio
Recibir de cada Institución el listado de los oficiales de enlace de la PNP y del CC.FF.AA., designados por cada Institución y comunicados a la ONPE.	Gerente de OSDN o quien delegue	---

	PROCEDIMIENTO	Código:	PR01-OSDN/SP
ONPE		Versión:	02
	SEGURIDAD DEL PROCESO ELECTORAL	Página:	4 de 21

7. DESARROLLO:

7.1. Elaboración de Disposiciones e instrucciones en materia de seguridad

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
Elaborar proyecto de las Disposiciones para garantizar el orden, la seguridad y la libertad personal durante los procesos electorales. Nota: Se puede tomar como referencia las disposiciones de la última elección de similares características.	Gerente de OSDN o quien delegue	----
Remitir los proyectos de las Disposiciones e instrucciones, la Resolución para su aprobación y el Informe a la Jefatura Nacional. Nota: Realizar correcciones en caso lo solicite la JN.	Gerente de OSDN o quien delegue	Informe
Elaborar oficios para la remisión de las Disposiciones aprobadas a la Secretaría General del Ministerio Público, al Jefe del Comando Conjunto de las Fuerzas Armadas y al Director General de la Policía Nacional del Perú. [ ]	Gerente de OSDN o quien delegue	Oficio

7.2. Solicitud para designación de OE de la PNP y del CC.FF.AA.

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
[ ]	[ ]	[ ]
Emitir oficios dirigidos al Jefe del CC.FF.AA. y al Director General de la PNP, solicitando que se designe a los oficiales de enlaces de sus respectivas Instituciones ante la ONPE. Nota: Adjuntar a los oficios las publicaciones del diario oficial El Peruano, sobre la convocatoria a los procesos electorales.	Gerente de OSDN o quien delegue	Oficio
Recibir de cada Institución el listado de los oficiales de enlace de la PNP y del CC.FF.AA., designados por cada Institución y comunicados a la ONPE.	Gerente de OSDN o quien delegue	---

ONPE	PROCEDIMIENTO	Código:	PR01-OSDN/SP
		Versión:	02
	SEGURIDAD DEL PROCESO ELECTORAL	Página:	5 de 21

7.3. Elaboración de Contenidos de la Cartilla de Instrucción para los efectivos de la PNP y del FF.AA., y la Cartilla Informativa para los representantes del Ministerio Público

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
Para elaborar la Cartilla de Instrucción: Revisar la normativa vigente sobre las funciones, atribuciones y prohibiciones de los efectivos de las FF.AA. y de la PNP, en relación a sus facultades antes, durante y después a los procesos electorales. Para elaborar la **Cartilla Informativa**: Revisar la normativa vigente sobre las funciones, atribuciones y prohibiciones de los ciudadanos, miembros mesa, observadores, personeros y efectivos de la PNP y FF.AA.	Gerente de OSDN o quien delegue	---
Elaborar y remitir mediante Memorando, los proyectos de los contenidos de las Cartillas a la GAJ para su revisión y recomendaciones.	Gerente de OSDN o quien delegue	Memorando con los proyectos de los Contenidos de la Cartilla
Elaborar y remitir mediante Memorando, los contenidos de las Cartillas a la GIEE para su diagramación y diseño.	Gerente de OSDN o quien delegue	Memorando con los Contenidos de la Cartilla
Recibir de la GIEE la diagramación y diseño de las cartillas para revisión y V°B° final. En caso se identifiquen observaciones son informadas, a la GIEE para su corrección, de lo contrario brindar la conformidad, para el inicio de su impresión. [ ]	Gerente de OSDN	Memorando

7.4. Coordinación con otras entidades para recepción de información.

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
Identificar las instituciones que podrían contar con información valiosa que contribuya a la mejor organización de la seguridad de los procesos electorales. Tomando en cuenta la especial geografía del territorio nacional, la situación socio-política y demográfica y la época en la que se celebran los procesos electorales.	Gerente de OSDN o quien delegue	---
Oficiar a las instituciones que posean información que contribuyan a la organización	Gerente de OSDN o quien delegue	Oficios, de ser el caso.

ONPE	PROCEDIMIENTO	Código:	PR01-OSDN/SP
		Versión:	02
	SEGURIDAD DEL PROCESO ELECTORAL	Página:	5 de 21

7.3. Elaboración de Contenidos de la Cartilla de Instrucción para los efectivos de la PNP y del FF.AA., y la Cartilla Informativa para los representantes del Ministerio Público

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
Para elaborar la Cartilla de Instrucción: Revisar la normativa vigente sobre las funciones, atribuciones y prohibiciones de los efectivos de las FF.AA. y de la PNP, en relación a sus facultades antes, durante y después a los procesos electorales. Para elaborar la **Cartilla Informativa**: Revisar la normativa vigente sobre las funciones, atribuciones y prohibiciones de los ciudadanos, miembros mesa, observadores, personeros y efectivos de la PNP y FF.AA.	Gerente de OSDN o quien delegue	---
Elaborar y remitir mediante Memorando, los proyectos de los contenidos de las Cartillas a la GAJ para su revisión y recomendaciones.	Gerente de OSDN o quien delegue	Memorando con los proyectos de los Contenidos de la Cartilla
Elaborar y remitir mediante Memorando, los contenidos de las Cartillas a la GIEE para su diagramación y diseño.	Gerente de OSDN o quien delegue	Memorando con los Contenidos de la Cartilla
Recibir de la GIEE la diagramación y diseño de las cartillas para revisión y V°B° final. En caso se identifiquen observaciones son informadas, a la GIEE para su corrección, de lo contrario brindar la conformidad, para el inicio de su impresión. [ ]	Gerente de OSDN	Memorando

7.4. Coordinación con otras entidades para recepción de información.

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
Identificar las instituciones que podrían contar con información valiosa que contribuya a la mejor organización de la seguridad de los procesos electorales. Tomando en cuenta la especial geografía del territorio nacional, la situación socio-política y demográfica y la época en la que se celebran los procesos electorales.	Gerente de OSDN o quien delegue	---
Oficiar a las instituciones que posean información que contribuyan a la organización	Gerente de OSDN o quien delegue	Oficios, de ser el caso.

ONPE	PROCEDIMIENTO	Código:	PR01-OSDN/SP
		Versión:	02
	SEGURIDAD DEL PROCESO ELECTORAL	Página:	5 de 21

7.3. Elaboración de Contenidos de la Cartilla de Instrucción para los efectivos de la PNP y del FF.AA., y la Cartilla Informativa para los representantes del Ministerio Público

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
Para elaborar la Cartilla de Instrucción: Revisar la normativa vigente sobre las funciones, atribuciones y prohibiciones de los efectivos de las FF.AA. y de la PNP, en relación a sus facultades antes, durante y después a los procesos electorales. Para elaborar la **Cartilla Informativa**: Revisar la normativa vigente sobre las funciones, atribuciones y prohibiciones de los ciudadanos, miembros mesa, observadores, personeros y efectivos de la PNP y FF.AA.	Gerente de OSDN o quien delegue	---
Elaborar y remitir mediante Memorando, los proyectos de los contenidos de las Cartillas a la GAJ para su revisión y recomendaciones.	Gerente de OSDN o quien delegue	Memorando con los proyectos de los Contenidos de la Cartilla
Elaborar y remitir mediante Memorando, los contenidos de las Cartillas a la GIEE para su diagramación y diseño.	Gerente de OSDN o quien delegue	Memorando con los Contenidos de la Cartilla
Recibir de la GIEE la diagramación y diseño de las cartillas para revisión y V°B° final. En caso se identifiquen observaciones son informadas, a la GIEE para su corrección, de lo contrario brindar la conformidad, para el inicio de su impresión. [ ]	Gerente de OSDN	Memorando

7.4. Coordinación con otras entidades para recepción de información.

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
Identificar las instituciones que podrían contar con información valiosa que contribuya a la mejor organización de la seguridad de los procesos electorales. Tomando en cuenta la especial geografía del territorio nacional, la situación socio-política y demográfica y la época en la que se celebran los procesos electorales.	Gerente de OSDN o quien delegue	---
Oficiar a las instituciones que posean información que contribuyan a la organización	Gerente de OSDN o quien delegue	Oficios, de ser el caso.

ONPE	PROCEDIMIENTO	Código:	PR01-OSDN/SP
		Versión:	02
	SEGURIDAD DEL PROCESO ELECTORAL	Página:	7 de 21

DESCRIPCION DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
Enviar la información por medio de correo electrónico, en documento0s escritos o en cualquier otro medio, a los oficiales de enlace del CC.FF.AA., a la PNP, a Secretario General del MP y/o los PJFSDJ así como a los órganos de la Institución vinculados a la organización de los procesos electorales, si fuera pertinente, para el planeamiento interno de sus acciones.	Gerente de OSDN o quien delegue	---
Realizar reuniones de coordinación, con los OE designados por el CC.FF.AA. y la PNP, y según se requiera con representantes del MP o de las PJFSDJ, para verificar el avance de la organización del proceso electoral respecto a la seguridad del mismo, en atención a las disposiciones que en materia de seguridad aprueba la ONPE y al presente procedimiento, con motivo de los procesos electorales.	Gerente de OSDN o quien delegue	---
Coordinar con los OE de la PNP y del CC.FF.AA., los aspectos referidos a: - La protección y resguardo referente a: • Sedes centrales de la ONPE, JNE y del RENIEC. • Sedes de las ODPE, ORC y oficinas distritales, JEE y las oficinas del RENIEC. • Sedes en donde se encuentren los centros de cómputo y procesamiento de actas electorales. • Sedes donde se producen y/o custodian materiales electorales y/o Equipos informáticos Electorales. • Locales de votación. - Condiciones generales para la recepción del material electoral en los locales de votación y el repliegue del mismo. - La seguridad antes, durante y después de los procesos electorales, garantizando la libertad de los ciudadanos para ejercer su derecho al voto; así como a los miembros de mesa, personeros de organizaciones políticas, promotores y observadores para ejercer su función sin coacción alguna.	Gerente de OSDN o quien delegue	---
Coordinar mediante comunicaciones escritas o telefónicas con el MP o las PJFSDJ para que los Fiscales de Prevención del Delito o los Fiscales Provinciales y/o Mixtos desarrollen sus funciones durante la	Gerente de OSDN o quien delegue	---

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
organización de los procesos electorales.		

7.6. Coordinación con PNP para el resguardo del material de sufragio durante despliegue y repliegue a nivel nacional.

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
Coordinar con la GGE y GOECOR, reuniones de trabajo para el resguardo de las unidades de transporte durante todo el trayecto que demande el despliegue y repliegue terrestre y aéreo del material de sufragio y equipos informáticos a cada ODPE u ORC y viceversa.	Gerente de OSDN o quien delegue	---
El resguardo del despliegue del material de sufragio de la ODPE u ORC a los locales de votación se detalla en el IN01-OSDN/SP Seguridad en el Despliegue y Repliegue, según PR01-GGE/DMS Despliegue de material de sufragio y PR01-GGE/RME Repliegue de material electoral y equipos Informáticos y documentos electorales.	Gerente de OSDN o quien delegue	Itinerario de rutas despliegue y repliegue
Recibir de la GGE, el Itinerario y rutas de despliegue y repliegue. Nota: De ser el caso, la GGE comunica a la GOECOR y a la OSDN las modificaciones que se presenten en el itinerario de rutas de despliegue y repliegue como máximo con 48 horas de anticipación respecto a la fecha programada, producto de variables externas, tales como: condiciones climáticas, condiciones de seguridad, interrupción de vías de comunicación, etc.	Gerente de OSDN o quien delegue	--
Recepcionar y coordinar el orden de salida de los vehículos policiales que custodiarán las unidades de transporte del material electoral y equipos informáticos, el día programado para el despliegue y repliegue.	GGE (En Lima) / JODPE, coordinador de ORC o quien haga sus veces	---

	PROCEDIMIENTO	Código:	PR01-OSDN/SP
ONPE		Versión:	02
	SEGURIDAD DEL PROCESO ELECTORAL	Página:	9 de 21

DESCRIPCION DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
Iniciar el despliegue y repliegue del material de sufragio y equipos informáticos, de acuerdo al Itinerario de fechas, horas y destino final entregado al representante de cada área de la PNP. **NOTA:** a) Cada unidad de transporte deberá estar acompañado por un vehículo policial que lo custodiará hasta el límite de su jurisdicción, siendo reemplazado por otro vehículo policial que lo escoltará hasta el término de su jurisdicción, así sucesivamente hasta la llegada del vehículo a la ODPE u ORC. b) En el caso en que el proceso electoral se lleve a cabo en Lima Metropolitana y/o Callao, el despliegue del material electoral se realiza desde el local de distribución administrado por la GGE hacia los locales de votación, contando durante todo su trayecto con custodia policial (despliegue y repliegue)	GGE (En Lima) / JODPE, coordinador de ORC o quien haga sus veces	---
Coordinar con PNP y/o FFAA para despliegue y repliegue del material sufragio y equipos informáticos desde la ODPE u ORC hacia los Locales de Votación, según indicaciones brindadas por la GOECOR según instructivo IN01-OSDN/SP Seguridad en el despliegue y repliegue.	JODPE o el coordinador de la ORC o quien haga sus veces	---

7.7. Coordinaciones de las ODPE u ORC en cada jurisdicción:

DESCRIPCION DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
Realizar las actividades de seguridad según lo indicado en el Anexo 7 Protocolo de Seguridad para las ODPE u ORC	JODPE / coordinador de ORC o quien haga sus veces	-

ONPE	PROCEDIMIENTO	Código:	PR01-OSDN/SP
		Versión:	02
	SEGURIDAD DEL PROCESO ELECTORAL	Página:	10 de 21

7.8. Otras Coordinaciones a realizar por la ODPE u ORC:

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	REGISTRO
7.8.1. Coordinación en caso de Problemas con el despliegue y repliegue Se realiza según el IN02-OSDN/SP Contingencia para Problemas en el Despliegue y Repliegue del material sufragio y equipos informáticos. **7.8.2. Coordinación en caso de Presentarse contingencias en las sedes de la ODPE y ORC** En caso de presentarse las siguientes contingencias en los locales de la ODPE u ORC: Inundación, problemas con el fluido eléctrico, emergencias de salud con el personal de la ODPE u ORC, actos delictivos e incendios; adoptar las medidas preventivas y correctivas, según el OD01-OSDN/SP Contingencias en las sedes de la ODPE y ORC. **7.8.3. Coordinación en caso de Ocurrencia de conmoción social** En caso de la ocurrencia de situaciones de conmoción social en la circunscripción de la ODPE u ORC, adoptar las medidas preventivas y correctivas según el OD02-OSDN/SP: Ocurrencia de conmoción social. **7.8.4. Coordinación en caso de presentarse Desastres Naturales.** En caso de presentarse desastres naturales en la circunscripción de la ODPE u ORC que pongan en riesgo la organización de los procesos electorales, de referéndum y otras consultas populares, adoptar las medidas preventivas y correctivas según el OD03-OSDN/SP: Acciones a considerar en caso de desastres naturales.	JODPE o el coordinador de la ORC o quien haga sus veces	

8. ANEXOS:

8.1. Anexo 1: Diagrama de Flujo de Elaboración de Disposiciones e instrucciones en materia de seguridad.
8.2. Anexo 2: Diagrama de Flujo de la solicitud de designación de OE de la PNP y del CC.FF.AA.
8.3. Anexo 3: Diagrama de Flujo de la elaboración de Contenidos de la Cartilla de Instrucción para los efectivos de la PNP y del FF.AA., y la Cartilla Informativa para los representantes del Ministerio Público.
8.4. Anexo 4: Diagrama de Flujo de Coordinación con otras entidades para recepción de información.
8.5. Anexo 5: Diagrama de Flujo de Coordinación de seguridad a nivel nacional.
8.6. Anexo 6: Diagrama de Flujo de Coordinación con PNP para el resguardo del material de sufragio durante despliegue y repliegue a nivel nacional.
8.7. Anexo 7: Protocolo de Seguridad para las ODPE u ORC

PROCEDIMIENTO	Código:	PR01-OSDN/SP
	Versión:	02
SEGURIDAD DEL PROCESO ELECTORAL	Página:	12 de 21
DOCUMENTO EN ESTUDIO		

Anexo 1: Diagrama de Flujo de Elaboración de Disposiciones e instrucciones en materia de seguridad

PR01-OSDN/SP-Seguridad del Proceso Electoral

ONPE	PROCEDIMIENTO	Código:	PR01-OSDN/SP
		Versión:	02
	SEGURIDAD DEL PROCESO ELECTORAL	Página:	13 de 21

Anexo 2: Diagrama de Flujo de la solicitud de designación de OE de la PNP y del CC.FF.AA.

PR01-OSDN/SP: Seguridad del Proceso Electoral

ONPE	PROCEDIMIENTO	Código:	PR01-OSDN/SP
		Versión:	02
	SEGURIDAD DEL PROCESO ELECTORAL	Página:	14 de 21

Anexo 3: Diagrama de Flujo de Elaboración de Contenidos de la Cartilla de Instrucción para los efectivos de la PNP y del FF.AA., y la Cartilla Informativa para los representantes del Ministerio Público

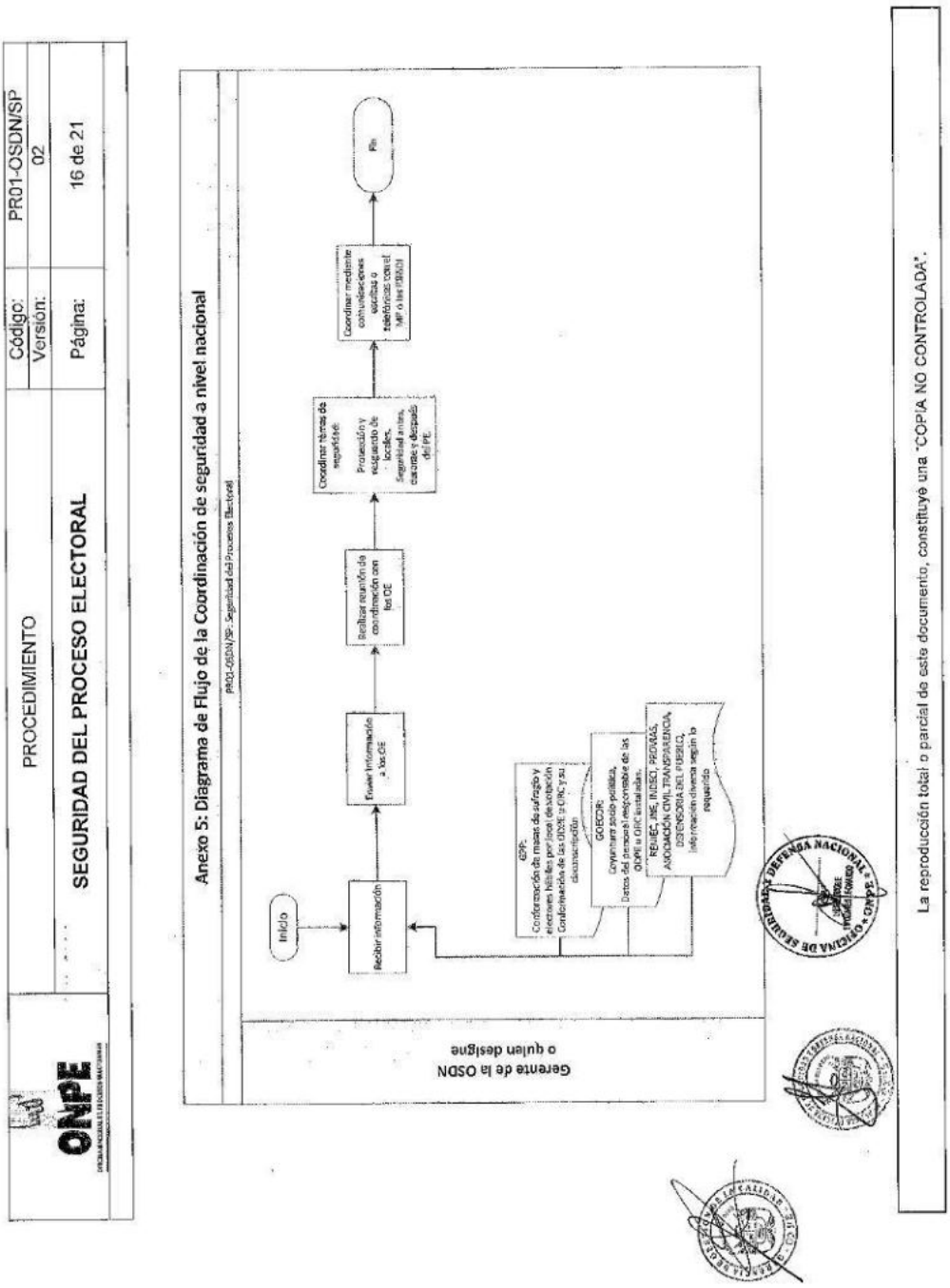
PR01-OSDN/SP: Seguridad del Proceso Electoral

La reproducción total o parcial de este documento, constituye una "COPIA NO CONTROLADA".

	PROCEDIMIENTO	Código:	PR01-OSDN/SP
ONPE		Versión:	02
	SEGURIDAD DEL PROCESO ELECTORAL	Página:	15 de 21

Anexo 4: Diagrama de Flujo de Coordinación con otras entidades para recepción de información

PR01-OSDN/SP: Seguridad del Proceso Electoral



ONPE	PROCEDIMIENTO	Código:	PR01-OSDN/SP
		Versión:	02
	SEGURIDAD DEL PROCESO ELECTORAL	Página:	17 de 21

Anexo 6: Diagrama de Flujo de Coordinación con PNP para el resguardo del material de sufragio durante despliegue y repliegue a nivel nacional

PR01-OSDN/SP- Seguridad del Proceso Electoral

Gerente de la OSDN o quien designe

SGOE de la GGE (En Lima) / JODPE, coordinador de ORC o quien haga sus veces

Inicio

Coordina reuniones de trabajo con el SGOE de GGE

Remisión de rutas de despliegue y repliegue

Asigna vehículos policiales

DESPLIEGUE

REPLIEGUE

Fin

La reproducción total o parcial de este documento, constituye una "COPIA NO CONTROLADA".

Anexo 7: Protocolo de Seguridad para las ODPE y ORC

Responsable: JODPE / coordinador de ORC o quien haga sus veces

ACCIONES DE COORDINACIÓN

1. Una vez instaladas las ODPE o designadas las ORC, los JODPE o Coordinadores de ORC, o quien haga sus veces, deberán presentarse con las autoridades de la zona, vinculadas al proceso electoral: PNP, FF.AA y MP, Gobernador; entre otros, manteniendo los adecuados niveles de coordinación y comunicación, elaborando el directorio telefónico correspondiente para casos de emergencia y ponerlo en conocimiento a la OSDN.
2. Informarse de asambleas, reuniones y acuerdos de organizaciones, gremios y otros actores sociales, así como, de la situación político social que pudiera estar registrándose en la jurisdicción de su responsabilidad), relacionada con el orden público y seguridad ciudadana necesarios para garantizar el normal desarrollo de los procesos electorales y poner de conocimiento a la OSDN.
3. Coordinar en conjunto con la OSDN, los servicios de seguridad para las instalaciones de la ODPE, ORC y JEE, con el Comando local de la PNP. Para ello, solicitará el resguardo correspondiente, por escrito, y de manera personal, en caso de la no instalación del servicio de seguridad policial, dará cuenta al Jefe Policial de la jurisdicción policial dando cuenta del incumplimiento del servicio, novedad que deberá comunicar a la OSDN.
4. Los coordinadores de las ORC´S o quien haga de sus veces, coordinara con la PNP la seguridad para el despliegue y repliegue del material y equipos electorales, desde las ODPE u ORC hacia los locales de votación y viceversa, debiendo formular un Plan de rutas de cada jurisdicción con la PNP. Se deberá tener en consideración la situación político social que se presenta en cada distrito, (conflictos sociales, marchas, bloqueos de vías, huelgas, siniestros, problemática del tránsito vehicular, etc.) así como los riesgos de seguridad (zonas críticas de incidencia delictiva, rutas de acceso a los locales de votación), que se puedan presentar durante los desplazamientos, debiendo comunicar a la OSDN los acuerdos tomados

5. Mantener permanente comunicación con la PNP para alertar sobre retrasos o reprogramación del inicio de los desplazamientos, coordinando los aspectos de detalle con las unidades operativas de la PNP que brindaran el servicio policial, poniendo en conocimiento a la OSDN.
6. Promover y/o solicitar reuniones de trabajo entre los representantes de la ODPE u ORC, JEE, MP, PNP, FF.AA, para coordinar los requerimientos de seguridad necesarios que garanticen el normal desarrollo del proceso electoral, de acuerdo a las competencias funcionales y legales de cada uno de las Instituciones, poniendo en conocimiento a la OSDN.
7. Recabar información del MP, PNP, FF.AA., así como de los actores políticos y sociales, a fin de tomar conocimiento de la coyuntura político electoral que pueda afectar la seguridad y el normal desarrollo de los procesos electorales, poniendo en conocimiento a la OSDN.
8. Establecer mecanismos de información con los medios de comunicación local a fin de desarrollar campañas informativas para sensibilizar al electorado, sobre las funciones y responsabilidades de los organismos del sistema electoral (ONPE, JNE y RENIEC), sobre el sufragio y escrutinio, así como para generar una corriente de opinión de respeto de los procesos y resultados electorales.
9. Elaborar un informe de seguridad de los locales de votación determinando las carencias estructurales: tipos de puertas de acceso, tipo de techo, sistema de iluminación, cantidad de accesos, vulnerabilidad de la instalación (cerco perimétrico, vallas de seguridad), así como el croquis de los locales de votación, poniendo en conocimiento a la OSDN.

ASPECTOS DE SEGURIDAD

1. Seguridad de locales e instalaciones de las ODPE y ORC.

1.1. Implementar medidas de seguridad básicas:

- Elaborar un Plan de Contingencia, en caso sea necesario evacuar las sedes de las ODPE u ORC, ante la inminente ocurrencia de incidentes de violencia, el mismo que deberá contener, por lo menos:
  a) La identificación de las vulnerabilidades de la sede.
  b) La identificación del o los accesos y salidas,
  c) El diseño de ruta de escape,
  d) Los puntos y horas de encuentro del personal evacuado.
- Contar con equipamiento básico de seguridad:
  a) Extintores: de agua, gas carbónico y oxígeno.
  b) Luces de Emergencia
  c) Señalización

1.2. Evitar proporcionar a extraños información relacionada con las medidas y niveles de seguridad establecidas.
1.3. Disponer que el personal contratado posea su identificación a la vista e indumentaria en todo momento del desempeño de sus labores.
1.4. Revisar que la sede o subsedes de la ODPE u ORC, cuenten con las medidas básicas de seguridad en su estructura (paredes, puertas, cerraduras, techos, entre otros), que cuente con ambientes que permitan albergar y resguardar al personal, material y equipos, además de disponer de los servicios de agua, desagüe y luz.
1.5. Verificar que en los locales de votación existan ambientes que permitan albergar y resguardar al personal, a los miembros de mesa, a los equipos y al material electoral.
1.6. Elaborar planes de contingencia para la evacuación y atención del personal del local de la ODPE u ORC.
1.7. Coordinar con la PNP los servicios de seguridad de las instalaciones antes, durante y después del proceso electoral.

i. Adoptar medidas de seguridad para la protección del local y evacuación del personal.
ii. 7.2 Disponer que el personal no participe bajo ninguna circunstancia en asambleas o reuniones organizadas por actores sociales.
iii. De haber enfrentamientos y disparos en la calle, nunca se asome por las ventanas, aléjese de las mismas y muévase arrastrándose por el piso hasta el punto de concentración, previamente definido.
iv. Coordinar con el personal de la ODPE u ORC para que cambien sus rutas de desplazamientos, y recomendar que se movilicen en grupos y por avenidas centrales.

En caso de realizarse manifestaciones frente a los locales de las ODPE u ORC y JEE:

v. Al tomarse conocimiento de posibles traslados de manifestantes a las sedes institucionales, solicitar el apoyo policial de la jurisdicción correspondiente.
vi. Disponer el cierre de los accesos a las instalaciones y la evacuación de personal no indispensable, el cual no deberá portar logos institucionales que lo hagan identificable, a fin de evitar agresiones por parte de terceros.
vii. Extremar las medidas de seguridad con los equipos informáticos y material electoral bajo su responsabilidad.
viii. Establecer comunicación con los manifestantes siempre y cuando se cuente con la custodia policial correspondiente.
ix. Ante manifestaciones violentas o pacíficas, mantener la calma y serenidad, identificar posibles instigadores, analizar la procedencia de los reclamos, informando sobre la legalidad o estado del reclamo, evitando entrar en enfrentamientos verbales que puedan exacerbar a los manifestantes.
x. En caso de grave alteración del orden público que afecte la seguridad de las instalaciones, material electoral, equipos informáticos y del personal, se deberá evacuar el local.

xi. Se deberá tener especial atención al material electoral crítico y no procesado, el cual deberá ser protegido y retirado con la seguridad correspondiente.

2. Seguridad de Locales de Votación

2.1. Incorporar como buena práctica que los efectivos de la PNP y la FF.AA., y el personal de la ONPE y del JEE, se reúnan en cada local de votación, al inicio del proceso electoral para repasar la Cartilla de Instrucción.
2.2. El Coordinador de Local de votación o quien haga sus veces, deberá presentarse con el oficial de las FF.AA a cargo de la patrulla; asimismo, con el efectivo policial de mayor rango que estará custodiando los exteriores de los locales de votación.
2.3. El personal de la PNP cumple una función de seguridad externa, no necesariamente de orientación a los electores, debido a que ello conlleva a distraer su responsabilidad de seguridad de los exteriores en los locales de votación.

2.4. En el personal de los organismos electorales, deben coordinar con el Jefe de la seguridad interna y externa (CC.FF.AA), a fin de unificar procedimientos para garantizar la máxima seguridad para la instalación de las mesas, inicio del proceso y término del proceso, garantizando la continuidad del escrutinio.
2.5. Coordinar con la FF.AA. y PNP la seguridad del material electoral, equipos informáticos y en especial de las actas electorales.
2.6. En caso de interrupción del proceso del escrutinio solicitar los refuerzos necesarios para su restablecimiento, debiendo solicitar al personal de la FF.AA. la seguridad correspondiente para garantizar la intangibilidad del material electoral y de los equipos informáticos.

2.7. Elaborar planes de contingencia para la evacuación del personal del local de la ODPE u ORC y de los locales de votación.
2.8. Informar a todas las instituciones de observación electoral para que conozcan de la situación.
2.9. Coordinar, de ser el caso, con la PNP para que apoyen en la instalación de las mesas de votación, ante la ausencia de miembros titulares y suplentes. Su apoyo en esta circunstancia es solo presencial y disuasiva.
2.10. Prever mayor número de carteles de resultados de contingencia, para evitar especulaciones por carteles siniestrados.

NOTA IMPORTANTE: Para los locales de votación que cuenten con punto de transmisión, este ambiente deberá contar con presencia de personal de las FFAA y se deberá indicar que el ingreso es SOLO PARA PERSONAL AUTORIZADO.

Anexo G IN01-OSDN/SP SEGURIDAD EN EL DESPLIEGUE Y REPLIEGUE

	INSTRUCTIVO	Código:	IN01-OSDN/SP
ONPE		Versión:	02
	SEGURIDAD EN EL DESPLIEGUE Y REPLIEGUE	Página:	1 de 6

Elaborado por:	Revisado por:	Aprobado por:
Firmado digitalmente por SIFUENTES LEONARDO Luis Enrique (FAU20291973851) Motivo: Soy el autor del documento Fecha: 29.12.2016 09:51:09 -05:00	Firmado digitalmente por LOPEZ VILLAFUERTE Fernando (FAU20291973851) Motivo: Soy el autor del documento Fecha: 03.01.2017 16:32:00 -05:00	Firmado digitalmente por LOPEZ VILLAFUERTE Fernando (FAU20291973851) Motivo: Soy el autor del documento Fecha: 03.01.2017 16:32:21 -05:00
Especialista en Seguridad y Defensa Nacional	Gerente de la Oficina de Seguridad y Defensa Nacional	Gerente de la Oficina de Seguridad y Defensa Nacional
	Firmado digitalmente por MOLINA VILCHEZ Jaime Enrique (FAU20291973851) Motivo: Doy V° B° Fecha: 29.12.2016 15:09:55 -05:00	
	Gerente de Gestión de la Calidad	

1. **OBJETIVO:**
   Establecer la secuencia de tareas a desarrollar para garantizar las condiciones de seguridad en el despliegue y repliegue del material de sufragio y equipos informáticos desde las sedes de las ODPE´S u ORC´S hasta los locales de votación y viceversa y desde el local de producción (GGE) hasta los locales de votación y viceversa de Lima Metropolitana y Callao.

2. **BASE NORMATIVA:**
   2.1. Artículo 179° de la Ley Orgánica de Elecciones.
   2.2. Artículo 27° de la Ley Orgánica de la Oficina Nacional de Procesos Electorales.

   Nota: Los documentos mencionados son los vigentes incluyendo sus modificaciones.

3. **REFERENCIAS:**
   3.1. PR01-OSDN/SP Seguridad de los procesos electorales

   Nota: Los documentos mencionados son los vigentes incluyendo sus modificaciones.

4. **DEFINICIONES Y ABREVIATURAS:**

   4.1. Definiciones:

N°	Término	Definición
-	-	-

   4.2. Abreviaturas:

N°	Término	Abreviatura
1	Coordinador de local de votación	CLV
2	Fuerzas Armadas.	FF.AA.
3	Jefe de ODPE	JODPE
4	Locales de votación.	LV
5	Mesa de sufragio	MS
6	Policía Nacional del Perú.	PNP
7	Oficina Nacional de Procesos Electorales.	ONPE
8	Oficina de Seguridad y Defensa Nacional	OSDN
9	Oficina Regional de Coordinación	ORC

ONPE	INSTRUCTIVO	Código:	IN01-OSDN/SP
		Versión:	02
	SEGURIDAD EN EL DESPLIEGUE Y REPLIEGUE	Página:	2 de 6

5. **DESARROLLO:**

5.1. Antes del Despliegue y/o Repliegue desde las ODPE´S u ORC´S hasta los LV y viceversa.

N°	Descripción de la tarea	Responsable	Registro generado
1	Recibir de la GGE, la siguiente información: 1 La fecha para el despliegue de materiales y equipos electorales a las ODPE´S y ORC´S provincias. 2 El itinerario o cronograma de despliegue indicando las rutas programadas e información de variables externas como: condiciones climáticas, interrupción de vías de comunicación, entre otras que guarden relación con la seguridad del desplazamiento de materiales y equipos electorales. 3 Información de los comisionados y choferes /teléfonos y número de placa de los vehículos con una anticipación de 72 horas.	Gerente de la OSDN o a quien delegue	SGD o correo electrónico
2	Recibir de la GOECOR, la siguiente información: 1 El reporte de la cantidad de LV y MS por distrito, provincias, ODPE u ORC y departamento. 2 El itinerario de despliegue de equipos y material electoral desde las ODPE´S u ORC´S hacia los locales de votación	Gerente de la OSDN o a quien delegue	SGD o correo electrónico
3	Remitir la información a la PNP y FFAA, a fin de que se tome conocimiento y se planifique el resguardo correspondiente.	Gerente de la OSDN, o a quien se delegue	Oficio o correo electrónico
4	Formular, con apoyo de la PNP, un Plan de Rutas, definiendo la ruta principal y la alterna, teniendo en consideración factores como: la situación político social que se presenta en cada distrito, conflictos sociales, marchas, bloqueos de vías, huelgas, siniestros, problemáticas del tránsito vehicular, etc., así como de los riesgos de seguridad (zonas críticas de incidencia delictiva, rutas de acceso a los LV), que se puedan presentar durante los desplazamientos. Nota: Contenido mínimo del Plan de Rutas: • Cantidad de vehículos • Número de placa de los vehículos • Nombres y Apellidos, números telefónicos de los comisionados y choferes. Remitir el Plan de Rutas la GOECOR y a la OSDN.	JODPE o Gestor de la ORC o quien haga sus veces	Plan de Rutas / SGD o correo electrónico
5	Remitir el Plan de Rutas al oficial de enlace de la PNP y FFAA, para su conocimiento y validación	Gerente de la OSDN, o a quien se delegue	Oficio o correo electrónico
6	Realizar, en coordinación con la OSDN, reuniones con los oficiales PNP y FFAA coordinadores de su Región y con los representantes de las entidades del sector público y privado que intervienen (energía, INDECI, bomberos, Ministerio Publico, RENIEC, JEE, entre otros), a fin de tratar temas	JODPE o Gestor de la ORC o quien haga sus veces	SGD o correo electrónico / Invitaciones / Actas

ONPE	INSTRUCTIVO	Código:	IN01-OSDN/SP
		Versión:	02
	SEGURIDAD EN EL DESPLIEGUE Y REPLIEGUE	Página:	3 de 6

N°	Descripción de la tarea	Responsable	Registro generado
	relacionado con la seguridad del proceso electoral, tales como: coyuntura socio política de las zonas, determinar las horas y fechas de inicio y termino del despliegue y repliegue del material electoral. Remitir las invitaciones y actas de los acuerdos a la GOECOR y a la OSDN.		
7	Remitir los acuerdos al oficial de enlace de la PNP y FFAA, para su conocimiento y validación.0.	Gerente de la OSDN, o a quien se delegue	Oficio o correo electrónico
8	Mantener permanente comunicación con los oficiales coordinadores de la PNP, a fin de coordinar la programación del inicio de los desplazamientos, la sincronización con las unidades operativas de la PNP, que brindaran el resguardo policial, poniendo en conocimiento a la GOECOR y OSDN.	JODPE o Gestor de la ORC o quien haga sus veces	SGD o correo electrónico

5.2. Antes del Despliegue y/o Repliegue desde el local de producción (GGE) hasta los LV y viceversa de Lima Metropolitana y Callao

N°	Descripción de la tarea	Responsable	Registro generado
1	Recibir de la GGE, la siguiente información: 1 La fecha para el despliegue de materiales y equipos electorales desde el local de producción (GGE) a los locales de votación Lima Metropolitana y Callao. 2 El itinerario o cronograma de despliegue indicando las rutas programadas e información de variables externas como: interrupción de vías de comunicación, entre otras que guarden relación con la seguridad del desplazamiento de materiales y equipos electorales. 3 Información de los comisionados y choferes /teléfonos y número de placa de los vehículos con una anticipación de 72 horas.	Gerente de la OSDN o a quien delegue	SGD o correo electrónico
2	Remitir la información a la PNP, a fin de que se tome conocimiento y se planifique el resguardo correspondiente.	Gerente de la OSDN, o a quien se delegue	Oficio o correo electrónico
3	Coordinar con la PNP, la asignación de patrulleros para resguardar a los vehículos que trasladen los equipos y materiales electorales.	Gerente de la OSDN, o a quien se delegue	--

5.3. Durante el Despliegue y/o Repliegue desde las ODPE´S u ORC´S hasta los LV y viceversa

N°	Descripción de la tarea	Responsable	Registro generado
1	Autorizar el inicio del despliegue y el repliegue del material de sufragio y equipos electorales sólo si los efectivos de la PNP o de las FFAA, acompañan su desplazamiento. Nota:	JODPE u Gestor de la ORC o quien haga sus veces	Vía telefónica o correo electrónico

	INSTRUCTIVO	Código:	IN01-OSDN/SP
ONPE		Versión:	02
	SEGURIDAD EN EL DESPLIEGUE Y REPLIEGUE	Página:	4 de 6

N°	Descripción de la tarea	Responsable	Registro generado
	En caso que los efectivos de la PNP y/o de las FFAA., no lleguen para iniciar el despliegue y el repliegue el JODPE o el Gestor de ORC se comunicará con el oficial coordinador de la Región a cargo, e inmediatamente informará de esta situación a la GOECOR y a la OSDN, por vía telefónica, mail o el medio disponible.		
2	Comunicar a los oficiales de enlace de la PNP o de las FFAA, a fin de que se priorice la llegada de los efectivos.	Gerente de la OSDN, o a quien se delegue	Vía telefónica o correo electrónico
3	Establecer rutas de contingencia en caso se presenten problemas en las rutas, según el IN02-OSDN/SP: Problemas con el despliegue y repliegue del material sufragio, el JODPE o el Gestor de la ORC se comunicará con el oficial coordinador de la Región, de la PNP y FFAA e inmediatamente informará de esta situación a la GOECOR y a la OSDN, por vía telefónica, mail o el medio disponible.	JODPE u Gestor de la ORC o quien haga sus veces	Vía telefónica o correo electrónico
4	Comunicar a los oficiales de enlace de la PNP o de las FFAA.	Gerente de la OSDN, o a quien se delegue	Vía telefónica o correo electrónico

5.4. Durante el Despliegue y/o Repliegue desde el local de producción (GGE) hasta los LV y viceversa de Lima Metropolitana y Callao

N°	Descripción de la tarea	Responsable	Registro generado
1	Autorizar el inicio del despliegue y el repliegue del material de sufragio y equipos electorales sólo si los efectivos de la PNP, acompañan su desplazamiento. Nota: En caso que los efectivos de la PNP y/o de las FFAA., no lleguen para iniciar el despliegue y el repliegue se deberá de poner en conocimiento al Centro de Control - CCTV de la OSDN.	Gerente GGE o quien haga sus veces	Vía telefónica o correo electrónico
2	Comunicar al oficial de enlace de la PNP, a fin de que se priorice la llegada de los efectivos.	Gerente de la OSDN, o a quien se delegue	Vía telefónica o correo electrónico
3	Realizara el monitoreo de los vehículos que transporta los equipos y materiales electorales, de presentarse alguna ocurrencia la misma será puesta en conocimiento al CCTV de la OSDN.	Personal de monitoreo de la SGOE, acorde el PR01-GGE/DMS	Vía telefónica o correo electrónico
4	Comunicar al oficial de enlace de la PNP, a fin de que se priorice el apoyo policial correspondiente.	Gerente de la OSDN, o a quien se delegue	Vía telefónica o correo electrónico

	INSTRUCTIVO	Código:	IN01-OSDN/SP
		Versión:	02
	SEGURIDAD EN EL DESPLIEGUE Y REPLIEGUE	Página:	5 de 6

5.5. Acciones específicas para el repliegue del material de sufragio y equipos informáticos desde los LV hasta las ODPE´S u ORC´S

N°	Descripción de la tarea	Responsable	Registro generado
1	Finalizado el escrutinio de votos en todas las mesas del local de votación, revisar que todo el personal de la ODPE u ORC se encuentre listo para replegarse, es decir, que hayan culminado el recojo y ordenamiento del material electoral, equipos informáticos y de los restos electorales.	CLV o quien haga sus veces	
2	Si durante el repliegue del material electoral y de los equipos informáticos, desde el local de votación hacia la sede de la ODPE u ORC, se produce un bloqueo de las vías, sea por desastre natural o por conmoción social, se deberá de coordinar las acciones con los oficiales responsables de la PNP y/o de las CC.FF.AA. que lo están custodiando, a fin de poner a buen recaudo al personal, material y equipos empleando la extracción del personal e informar al JODPE u Gestor de la ORC de la situación quienes pondrán en conocimiento a la GOECOR y a la OSDN.	Personal de la ODPE u ORC responsable del repliegue	Vía telefónica
3	Durante el trayecto de repliegue del local de votación hasta la ODPE correspondiente, mantener en todo momento, custodiado el material electoral y equipos informáticos.	Personal de la ODPE u ORC responsable del repliegue	
4	A su arribo a la sede de la ODPE u ORC, entregar el material electoral y equipos informáticos y firmar los cargos correspondientes.	Personal de la ODPE u ORC responsable del repliegue	--
5	Comunicar al oficial coordinador de la Región responsable de la PNP, a la GOECOR y a la OSDN, que el material electoral y los equipos informáticos, se encuentran en custodia de la ODPE u ORC, para que los efectivos de la PNP procedan a retirarse.	JODPE u Gestor de la ORC o quien haga sus veces	Vía telefónica

5.6. Acciones específicas para el repliegue del material de sufragio y equipos informáticos desde los LV de Lima Metropolitana y Callao hacia el local de producción (GGE)

N°	Descripción de la tarea	Responsable	Registro generado
1	Finalizado el escrutinio de votos en todas las mesas del local de votación, revisar que todo el personal de la ODPE u ORC se encuentre listo para replegarse, es decir, que hayan culminado el recojo y ordenamiento del material electoral, equipos informáticos y de los restos electorales.	CLV o quien haga sus veces	
2	Si durante el repliegue del material electoral y de los equipos informáticos, desde el local de votación hacia el local de producción (GGE), se produce un bloqueo de las vías, sea por desastre natural o por conmoción social, se deberá de coordinar las acciones con los oficiales responsables de la PNP, que lo están resguardando, a fin de poner a buen	Comisionado de GGE responsable del repliegue	Vía telefónica

N°	Descripción de la tarea	Responsable	Registro generado
	recaudo al personal, material y equipos empleando la extracción del personal e informar al CCTV de la OSDN.		
3	Se pondrá en conocimiento al Oficial de enlace de la PNP, a fin de que se refuerce el resguardo policial en el menor tiempo posible.	Gerente de la OSDN, o a quien se delegue	
4	Realizara el monitoreo de los vehículos que transporta los equipos y materiales electorales, de presentarse alguna ocurrencia la misma será puesta en conocimiento al CCTV de la OSDN.	Personal de monitoreo de la SGOE, acorde el PR01-GGE/DMS	Vía telefónica o correo electrónico

6. ANEXOS

No aplica

7. CUADRO DE CONTROL DE CAMBIOS

Versión anterior	Fecha de aprobación	Sección / Ítem	Categoría N: nuevo M: Modificado E: Eliminado	Principales cambios realizados con respecto a la versión anterior
01	05/02/2015	1	M	Se ha incluido el tramo desde el local de producción de la GGE hasta los LV en Lima Metropolitana y Callao
01	05/02/2015	5.1	M	Se hace referencia al tramo desde las ODPEs u ORCs hasta los LV. Precisiones en cuanto a la información entregada por GOECOR y la GGE
01	05/02/2015	5.2	E	Se eliminan las actividades en el caso de uso de rutas de emergencia.
01	05/02/2015	5.2	N	Se incluyen las tareas a realizarse antes del despliegue / repliegue desde el local de producción hasta los LV de Lima Metropolitana y Callao
01	05/02/2015	5.3	E	Se eliminan las acciones específicas para el repliegue de material de sufragio y equipos informáticos.

ANEXO H IN 02-OSDN/SP ACCIONES DE CONTINGENCIA PARA PROBLEMAS DURANTE EL DESPLIEGUE Y REPLIEGUE DEL MATERIAL DE SUFRAGIO

	INSTRUCTIVO	Código:	IN02-OSDN/SP
		Versión:	02
	ACCIONES DE CONTINGENCIA PARA PROBLEMAS DURANTE EL DESPLIEGUE Y REPLIEGUE DEL MATERIAL SUFRAGIO	Página:	1 de 4

Elaborado por:	Revisado por:	Aprobado por:
Especialista en Seguridad y Defensa Nacional	Gerente de la Oficina de Seguridad y Defensa Nacional Gerente de Gestión de la Calidad	Gerente de la Oficina de Seguridad y Defensa Nacional

1. **OBJETIVO:**
   Establecer las tareas que debe desarrollar el personal de la ONPE para facilitar la adopción de medidas preventivas y correctivas, en caso de ocurrencia de problemas en la seguridad durante el despliegue y repliegue del material de sufragio, equipos informáticos y documentos electorales, desde las ODPE´S u ORC´S hasta los locales de votación y viceversa y desde el local de producción (GGE) hasta los locales de votación y viceversa en Lima Metropolitana y Callao.

2. **BASE NORMATIVA:**
   No aplica.

3. **REFERENCIAS:**

   3.1. PR01-OSDN/SP Seguridad en los procesos electorales

   Nota: Los documentos mencionados son los vigentes incluyendo sus modificaciones.

4. **DEFINICIONES Y ABREVIATURAS:**

   4.1. Definiciones:

N°	Término	Definición
-	-	-

   4.2. Abreviaturas:

N°	Término	Abreviatura
1	Gerencia de Organización Electoral y Coordinación Regional	GOECOR
2	Jefe de la ODPE	JODPE
3	Ministerio Público	MP
4	Oficina Descentralizada de Procesos Electorales.	ODPE
5	Oficina Nacional de Procesos Electorales.	ONPE
6	Oficina de Seguridad y Defensa Nacional	OSDN
7	Oficina Regional de Coordinación	ORC
8	Policía Nacional del Perú.	PNP
9	Fuerzas Armadas	FFAA
10	Comando Conjunto de las Fuerzas Armadas	CCFFAA

5. DESARROLLO:

5.1 Desde las ODPE´S u ORC´S hasta los locales de votación y viceversa.

5.1.1. Actividades de Prevención

N°	Descripción de la tarea	Responsable	Registro generado
1	Planificar, proponer y validar las rutas principales y de contingencia con los oficiales coordinadores de cada Región de la PNP y FFAA poniendo en conocimiento a la GOECOR y a la OSDN.	JODPE o Gestor de la ORC o quien haga sus veces	Vía SGD o correo electrónico
2	Remitir la información a los oficiales de enlace de la PNP y CCFFAA, para su conocimiento y fines.	Gerente de la OSDN o a quien se delegue	Oficio o correo electrónico
3	Solicitar al CCFFAA, PNP y Defensoría del Pueblo, informes socio político y/o coyuntura social, en las Regiones y distritos donde se lleve a cabo el proceso electoral.	Gerente de la OSDN o a quien se delegue	Oficio o correo electrónico
4	Remitir la información proporcionada a las ODPE´S, ORC´S y GOECOR para las acciones correspondientes.	Gerente de la OSDN o a quien se delegue	Vía SGD o correo electrónico
5	Establecer juntamente con los oficiales encargados de la PNP y FFAA un plan de contingencia ante eventualidades o emergencias, estableciendo rutas de escape y puntos de extracción, poniendo en conocimiento a la GOECOR y a la OSDN.	Personal de la ODPE u ORC	Vía SGD o correo electrónico
6	Remitir la información a los oficiales de enlace de la PNP y CCFFAA, para su conocimiento y fines.	Gerente de la OSDN o a quien se delegue	Oficio o correo electrónico

5.1.2. En caso de ocurrencia

N°	Descripción de la tarea	Responsable	Registro generado
1	Ejecutar juntamente con los efectivos de la PNP o FFAA el plan de contingencia elaborado, comunicando inmediatamente al JODPE, Gestor de la ORC, a fin de que el mismo ponga en conocimiento a la GOECOR y a la OSDN.	Personal de la ODPE u ORC	Vía telefónica
2	Trasladar la información proporcionada a los oficiales de enlaces de la PNP o FFAA, según corresponda, para la adopción de las acciones correspondientes.	Gerente de la OSDN o a quien se delegue	Vía telefónica o correo electrónico

	INSTRUCTIVO	Código:	IN02-OSDN/SP
		Versión:	02
	ACCIONES DE CONTINGENCIA PARA PROBLEMAS DURANTE EL DESPLIEGUE Y REPLIEGUE DEL MATERIAL SUFRAGIO	Página:	3 de 4

5.1.3. Acciones posteriores

N°	Descripción de la tarea	Responsable	Registro generado
1	Colocar a buen recaudo al personal, material y equipos electorales, evaluar cuál es su condición e informar al JODPE, Gestor de la ORC, a fin de que el mismo ponga en conocimiento a la GOECOR y a la OSDN.	Personal de la ODPE u ORC	Vía telefónica
2	Trasladar la información proporcionada a los oficiales de enlaces de la PNP o FFAA, según corresponda, para la adopción de las acciones correspondientes.	Gerente de la OSDN o a quien se delegue	Vía telefónica o correo electrónico
3	Evaluar los planes de contingencia y las oportunidades de mejora juntamente con los oficiales encargados de la PNP y FFAA, poniendo en conocimiento del resultado de la evaluación a la GOECOR y a la OSDN.	JODPE o Gestor de la ORC o quien haga sus veces	----------
4	Elaborar el informe correspondiente y remitir a la GOECOR y a la OSDN.	JODPE o Gestor de la ORC o quien haga sus veces	Vía SGD o correo electrónico
5	Consolidar la información proporcionada y remitir a los oficiales de enlace de la PNP y CCFFAA.	Gerente de la OSDN o a quien se delegue	Oficio o correo electrónico

5.2 Desde el local de producción (GGE) hasta los locales de votación y viceversa de Lima Metropolitana y Callao.

5.2.1. Actividades de Prevención

N°	Descripción de la tarea	Responsable	Registro generado
1	Planificar y proponer rutas principales y de contingencia, poniendo en conocimiento a la OSDN.	Gerente de la GGE o quien haga sus veces	Vía SGD o correo electrónico
2	Remitir la información al oficial de enlace de la PNP, para su conocimiento y fines.	Gerente de la OSDN o a quien se delegue	Oficio o correo electrónico
3	Solicitar al CCFFAA, PNP y Defensoría del Pueblo, informes socio político y/o coyuntura social, en los distritos de Lima Metropolitana y Callao, donde se lleve a cabo el proceso electoral.	Gerente de la OSDN o a quien se delegue	Oficio o correo electrónico
4	Remitir la información proporcionada a la GGE para las acciones correspondientes.	Gerente de la OSDN o a quien se delegue	Vía SGD o correo electrónico

5.2.2. En caso de ocurrencia

N°	Descripción de la tarea	Responsable	Registro generado
1	Ejecutar juntamente con los efectivos de la PNP que lo resguardan el plan de contingencia elaborado, comunicando inmediatamente a la GGE y al centro de control – CCTV de la OSDN.	Comisionado de la GGE o quien haga de sus veces	Vía telefónica
2	Poner en conocimiento del oficial de enlace de la PNP, la información para reforzar el resguardo policial.	Gerente de la OSDN o a quien se delegue	Vía telefónica o correo electrónico

5.2.3. Acciones posteriores

N°	Descripción de la tarea	Responsable	Registro generado
1	Colocar a buen recaudo al personal, material y equipos electorales, evaluar cuál es su condición e informar a la GGE, a fin de que el mismo ponga en conocimiento a la OSDN.	Comisionado de la GGE o quien haga de sus veces	Vía telefónica
2	Trasladar la información proporcionada al oficial de enlace de la PNP, para su conocimiento y fines.	Gerente de la OSDN o a quien se delegue	Vía telefónica o correo electrónico

6. ANEXOS

No aplica.

7. CUADRO DE CONTROL DE CAMBIOS

Versión anterior	Fecha de aprobación	Sección / Ítem	Categoría N: nuevo M: Modificado E: Eliminado	Principales cambios realizados con respecto a la versión anterior
01	05/02/2015	Encabezado	M	Ajuste en el título del documento: "Acciones de contingencia para problemas durante el despliegue y repliegue del material sufragio"
01	05/02/2015	1 Objetivo	M	Se agrega el tramo desde el local de producción (GGE) hacia los locales de votación de Lima Metropolitana y Callao.
01	05/02/2015	5 Desarrollo	M	Se ordena por tramos del despliegue y repliegue: 1° Desde las ODPE´S u ORC´S hasta los locales de votación y viceversa. 2° Desde el local de producción (GGE) hasta los locales de votación y viceversa de Lima Metropolitana y Callao.

ANEXO I FM01-OSDN/SP FORMATO DE ACTA REUNIÓN DE SEGURIDAD PARA EL PROCESO ELECTORAL

ONPE	**FORMATO**	Código:	FM01-OSDN/SP
		Versión:	01
	REUNIÓN DE COORDINACIÓN DE SEGURIDAD PARA EL PROCESO ELECTORAL	Fecha de aprobación:	08/03/2019
		Página:	1 de 2

PROCESO ELECTORAL: _____

ACTA N°.....-2019-ODPE...../ONPE

Lugar:		
Fecha:	Hora de inicio	Hora de termino

Temas a Tratar:

1.
2.
3.
4.

Desarrollo de la reunión:

[Relatar brevemente la sesión resaltando aquellos aspectos relevantes relacionados a los temas a tratar]

ONPE Firma Digital
Firmado digitalmente por CHUMBE GUTIERREZ Guillermo Alexander FAU 20291973851 soft
Motivo: Doy V° B°
Fecha: 08.03.2019 16:09:29 -05:00

ONPE Firma Digital
Firmado digitalmente por IGLESIAS AREVALO Walter Mauro FAU 20291973851 soft
Motivo: Doy V° B°
Fecha: 08.03.2019 16:50:03 -05:00

ONPE	**FORMATO**	Código:	FM01-OSDN/SP
		Versión:	01
	REUNIÓN DE COORDINACIÓN DE SEGURIDAD PARA EL PROCESO ELECTORAL	Fecha de aprobación:	08/03/2019
		Página:	2 de 2

Acuerdos:

N°	**Descripción del Acuerdo** *[Deberá definir una acción o actividad a ser realizada]*	**Responsable** (Institución / persona)	**Fecha de Implementación** *[Se refiere a la fecha que se deberá tener concluido o implementado el acuerdo]*
1			
2			
3			
4			
5			

Firman los participantes, dando fe del desarrollo de la reunión y de los acuerdos asumidos en señal de conformidad.

N°	Participante	Institución	Cargo	firma
1				
2				
3				
4				
5				
6				
7				
8				

ANEXO J OD01-OSDN/SP ACCIONES A IMPLEMENTAR PARA PREVENIR Y/O ATENDER CONTINGENCIAS POR EMERGENCIAS Y DESASTRES EN LAS SEDES DE LA ODPE Y ORC

	OTROS DOCUMENTOS	Código:	OD01- OSDN/SP
		Versión:	01
	ACCIONES A IMPLEMENTAR PARA PREVENIR Y/O ATENDER CONTINGENCIAS POR EMERGENCIAS Y DESASTRES EN LAS SEDES DE LA ODPE Y LAS ORC	Página:	1 de 14

Elaborado por:	Revisado por:	Aprobado por:
Firmado digitalmente por MUÑOZ ALTAMIRANO Amilkar (FAU20291973851) Motivo: Soy el autor del documento Fecha: 24.05.2018 08:43:57 -05:00	Firmado digitalmente por ROJO MANSILLA Daniel Ernesto (FAU20291973851) Motivo: Doy V° B° Fecha: 25.05.2018 15:24:17 -05:00	Firmado digitalmente por MORA ITO Alfredo FAU 20291973851 soft Motivo: Doy V° B° Fecha: 28.05.2018 12:41:22 -05:00
Especialista en Seguridad en Operaciones Electorales	Gerente de Organización Electoral y Coordinador Electoral Firmado digitalmente por PEREYRA VILLANUEVA Ivan FAU 20291973851 soft Motivo: Doy V° B° Fecha: 25.05.2018 15:24:17 -05:00 Gerente de Gestión de la Calidad	Gerente de la Oficina de Seguridad y Defensa Nacional

1. BASE LEGAL

DECRETO SUPREMO Nº 002-2018-PCM Nuevo Reglamento de Inspecciones Técnicas de Seguridad en Edificaciones

2. TÉRMINOS Y DEFINICIONES

2.1 Brigadas de emergencia
Grupos compuestos por personal con conocimiento en técnicas de control de emergencias.

2.2 Hurto
Delito que consiste en el apoderamiento ilegítimo de una cosa mueble, ajena en todo o en parte, sin usar la fuerza sobre las cosas, la violencia física en las personas, o la intimidación para obligar a la entrega.

2.3 Intrusión
Consiste en la entrada sin derecho a espacio ajeno mediante simulación o sigilo.

2.4 Robo
Delito que consiste en apropiarse ilícitamente de una cosa mueble, ajena en todo o en parte, haciendo uso de la violencia física en las personas, o la intimidación para obligar a la entrega.

2.5 Sabotaje
Acción deliberada, dirigida que tiene como objeto debilitar a un enemigo, mediante la subversión, la obstrucción, la interrupción o la destrucción.

	OTROS DOCUMENTOS	Código:	OD01- OSDN/SP
		Versión:	01
	ACCIONES A IMPLEMENTAR PARA PREVENIR Y/O ATENDER CONTINGENCIAS POR EMERGENCIAS Y DESASTRES EN LAS SEDES DE LA ODPE Y LAS ORC	Página:	2 de 14

3. Abreviaturas

N°	Abreviatura	Término
1	JODPE	Jefe de la ODPE
2	GOECOR	Gerencia de Organización Electoral y Coordinación Regional
3	OSDN	Oficina de Seguridad y Defensa Nacional
4	CO	Coordinador de Operaciones
5	CAODPE	Coordinador Administrativo de ODPE

4. DESARROLLO

4.1. Aspectos Generales (ODPE)

N°	Descripción de la tarea	Responsable
1	Designará a los responsables de las brigadas de Emergencia en ODPE. ▪ Jefe ODPE/Gestor ORC, Jefe de Brigada ▪ CAODPE/Asistente de Oficina: Brigadista de auxilio ▪ Coordinador de operaciones/Gestor ORC: Brigadista de Incendio ▪ Auxiliar diurno y nocturno/Asistente de Oficina: Brigadista de evacuación.	JODPE/ Gestor ORC
2	Remitir a través del SGD, informe a la GOECOR, con la relación de los brigadistas y los planos de distribución de zonas seguras.	JODPE/Gestor ORC
3	Remitir a OSDN la relación de brigadistas y los planos de distribución de zonas seguras.	GOECOR
4	Revisar y aprobar los planos de distribución de zonas seguras y emitir a GOECOR.	OSDN
5	Mantener implementado el botiquín de primeros auxilios, linterna portátil, radio a pilas portátil, teléfono, alimentos envasados y agua. Organizar un botiquín de primeros auxilios, y ubicarlo en un lugar visible. De preferencia, el botiquín, deberá contar con lo siguiente: ▪ **Materiales:** Suero fisiológico o Cloruro de Sodio (para el lavado de heridas), sales rehidratantes (Una cucharada de sal en un litro de agua), Agua oxigenada, Alcohol, Polividona Yodada o Betadine (antiséptico local externo), algodón y gasas estériles, esparadrapo antialérgico, venditas auto- adhesivas, vendas elásticas y jabón.	JODPE/Gestor ORC

	OTROS DOCUMENTOS	Código:	OD01- OSDN/SP
		Versión:	01
	ACCIONES A IMPLEMENTAR PARA PREVENIR Y/O ATENDER CONTINGENCIAS POR EMERGENCIAS Y DESASTRES EN LAS SEDES DE LA ODPE Y LAS ORC	Página:	3 de 14

N°	Descripción de la tarea	Responsable
	▪ **Medicamentos:** Ácido Aceptil Salicílico o Aspirina (dolor, inflamación, fiebre) Paracetamol o Panadol (dolor, inflamación, fiebre), Ibuprofeno o Dolomax (dolor, inflamación), Propinoxato o Plidán (Dolor abdominal, cólico estomacal), Clorfenamina o Cloroalergán (alergia, intoxicación), Dimenhidrinato o Gravol (náuseas, mareos, vómitos).	
6	Elaborar un directorio de números de emergencia y publicarlo	JODPE/Gestor ORC
7	Identificar y mantener actualizado un inventario de los equipos, mobiliario y material con que cuenta la ODPE u ORC.	JODPE/Gestor ORC

4.2. Acciones a implementar frente a casos de Inundación

N°	Descripción de la tarea	Responsable
1	Revisar periódicamente las tuberías de agua y desagüe ubicadas en los ambientes de la sede de la ODPE, de las oficinas distritales y de las ORC. Especialmente si cuenta con ambientes de varios niveles y registrarlo en el formato **Anexo 1.** Nota: En los ambientes cuyos techos no sean de concreto (como calaminas, tejas, planchas plastificadas, etc.) la revisión deberá realizarse en forma permanente	CO ODPE/Asistente ORC
2	Proceder inmediatamente al corte del fluido eléctrico (anule la llave de la caja principal).	CO ODPE/Asistente ORC
3	Usar lintemas de mano para la inspección de todos los ambientes que hubieran sido perjudicados por la inundación	Aux. diur/Noct
4	Desplazar el mobiliario, los equipos y el material electoral afectado a otros ambientes más seguros y secos.	Personal ODPE/ORC
5	Iniciar el retiro de las aguas empozadas con cubetas, esponjas y otros implementos que impidan un incremento acelerado del grado de humedad.	Personal ODPE/ORC
6	En caso de ser crítica la presencia del agua, solicitar apoyo de los Bomberos, para que desocupen el agua empozada	JODPE/ Gestor ORC
7	Activar las brigadas de emergencia.	JODPE/ Gestor ORC
8	Coordinar los primeros auxilios de ser necesario.	JODPE/ Gestor ORC

	OTROS DOCUMENTOS	Código:	OD01- OSDN/SP
		Versión:	01
	ACCIONES A IMPLEMENTAR PARA PREVENIR Y/O ATENDER CONTINGENCIAS POR EMERGENCIAS Y DESASTRES EN LAS SEDES DE LA ODPE Y LAS ORC	Página:	4 de 14

N°	Descripción de la tarea	Responsable
9	Evaluar daños y con la ayuda de Defensa Civil determinar si el local es aún habitable	JODPE/ Gestor ORC
10	Revisar cuidadosamente las instalaciones eléctricas a fin de verificar su funcionamiento	CO ODPE/Asistente ORC
11	Revisar cuidadosamente los equipos que estuvieron expuestos al agua, a fin de evitar o producir su mal funcionamiento en caso de ser encendidos	CAODPE/CO/ Gestor ORC
12	Si existe documentación y/o material electoral húmedo, para su recuperación, se deberá ▪ Ubicar la documentación en ambientes amplios y ventilados, evitando el contacto con los ambientes afectados por la inundación. ▪ Proceder al secado manual ▪ Separar, los documentos manchados de barro para limpiarlos mediante el enjuague correspondiente.	CAODPE/CO Gestor ORC
13	Informar inmediatamente, usando el medio más idóneo (teléfono, celular, correo electrónico, Etc.), a la GOECOR.	JODPE/ Gestor ORC

4.3. Acciones a implementar frente a casos de problemas o cortes del fluido eléctrico.

N°	Descripción de la tarea	Responsable
1	**Acciones Preventivas** ▪ Encargar o revisar periódicamente las instalaciones eléctricas del local para garantizar que estén en buen estado y registrarlo en el anexo 1. ▪ Si detecta conexiones en mal estado, interruptores defectuosos o tomacorrientes deteriorados, coordinar su reparación o cambio inmediato. ▪ Verificar o encargar la revisión para que los cables de los equipos de cómputo o eléctricos en uso estén en buen estado, y que sean los adecuados para la carga de su instalación. ▪ No sobrecargar las instalaciones eléctricas. La carga utilizada debe ser adecuada al circuito eléctrico de acuerdo al plano de distribución eléctrica. ▪ Evitar conectar muchos equipos a un solo tomacorriente.	CO ODPE/Asistente ORC
2	**En Caso de Ocurrencia** ▪ Ante el incendio de tipo eléctrico no use extintor de agua, emplee uno de gas carbónico o de polvo químico seco.	CO ODPE/Asistente ORC

	OTROS DOCUMENTOS	Código:	OD01- OSDN/SP
		Versión:	01
	ACCIONES A IMPLEMENTAR PARA PREVENIR Y/O ATENDER CONTINGENCIAS POR EMERGENCIAS Y DESASTRES EN LAS SEDES DE LA ODPE Y LAS ORC	Página:	5 de 14

N°	Descripción de la tarea	Responsable
	▪ Tratar de desconectar el circuito eléctrico desde el interruptor principal. ▪ Apagar equipos, bajar la llave general de luz ▪ Poner en funcionamiento la brigada de emergencia.	
3	**Acciones Posteriores** ▪ Reportar la ocurrencia a la GOECOR. ▪ Si el hecho es reciente, efectuar revisión general.	JODPE/ Gestor ORC

4.4. Acciones a implementar frente a casos de emergencias de Salud con el personal.

N°	Descripción de la tarea	Responsable
1	**En Caso de Ocurrencia** ▪ Comunicarse de inmediato con los servicios de emergencia. ▪ Actuar si se tiene la seguridad de lo que se va a hacer. Si existen dudas es preferible no hacer nada. ▪ Conservar la tranquilidad para actuar con serenidad y rapidez. Esto da confianza al lesionado. ▪ No retirarse del lado del lesionado. Si se encuentra solo, solicite la ayuda necesaria. ▪ Efectuar una revisión de la víctima, para descubrir lesiones distintas a la que motivó la atención y que no pueden ser manifestadas por ésta o sus acompañantes. ▪ De ser posible, hacer una identificación completa de la víctima, de sus acompañantes.	Personal de ODPE/ORC
2	**Acciones Posteriores** ▪ Reportar la emergencia de salud a la GOECOR.	JODPE/ Gestor ORC

4.5. Acciones a implementar frente a casos de ocurrencia de actos delictivos.

N°	Descripción de la tarea	Responsable
1	Entregar, mediante cargo, los bienes asignados a los LS.	CAODPE/ Gestor ORC
2	Verificar que el grado de seguridad de las puertas, ventanas y escritorios de cada ambiente sean los adecuados.	Personal de ODPE

N°	Descripción de la tarea	Responsable
3	Reportar inmediatamente la ocurrencia a la instancia competente	JODPE/ Gestor ORC
4	Reforzar las medidas de seguridad para que la situación no se repita.	JODPE/Gestor ORC

4.6. Acciones a implementar frente a casos de Sabotaje a la sede, o a los bienes muebles.

N°	Descripción de la tarea	Responsable
1	Restringir el acceso del personal no autorizado a los ambientes.	
2	Resguardar el uso y cuidado de los servicios básicos, de los equipos y material electoral	Auxiliar diurno y nocturno
3	Gestionar el apoyo de las FF.AA. o PNP para la seguridad externa del local.	JODPE/ Gestor ORC
4	Verificar que la iluminación perimétrica y externa ayude a la observación nocturna	JODPE/ Gestor ORC
5	Reportar inmediatamente la ocurrencia de un hecho a la instancia competente	JODPE/ Gestor ORC
6	Reportar el hecho mediante correo electrónico o llamada telefónica a la GOECOR, y a la OSDN.	JODPE/ Gestor ORC
7	Evaluar daños	JODPE/ Gestor ORC
8	Reunir al personal y reforzar las medidas de seguridad	JODPE/ Gestor ORC

4.7. Acciones a implementar frente a casos de Incendio.

N°	Descripción de la tarea	Responsable
1	Designar al CO y/o asistente de operaciones para que efectué la revisión y se evite lo siguiente: Evitar la acumulación de basura, en los ambientes. Evitar la sobrecarga de tomacorrientes de uso habitual. Evitar el uso de cables eléctricos parchados, viejos o deteriorados.	JODPE/ Gestor ORC

	OTROS DOCUMENTOS	Código:	OD01- OSDN/SP
		Versión:	01
	ACCIONES A IMPLEMENTAR PARA PREVENIR Y/O ATENDER CONTINGENCIAS POR EMERGENCIAS Y DESASTRES EN LAS SEDES DE LA ODPE Y LAS ORC	Página:	7 de 14

N°	Descripción de la tarea	Responsable
	Mantener orden y limpieza. Mantener los ambientes debidamente ventilados. No acumular material inflamable. Guardar los líquidos inflamables en lugar seguro.	
2	Distribuir adecuadamente los equipos de extinción de incendios. (Extintores, cajas de arena, depósitos de agua, mangueras); e instruir al personal sobre su uso adecuado	CAODPE/Gestor ORC
3	Colocar señalización en lugares visibles, como: no fumar, peligro alto voltaje, combustible, entre otros	CAODPE/Gestor ORC
4	Realizar simulacros de incendio según el anexo 2.	JODPE/ Gestor ORC
5	En el caso que el incendio sea controlable, proceda inmediatamente al corte del fluido eléctrico y del servicio de agua, y use los extintores idóneos o el material que cumpla igual función.	CO ODPE/Asistente ORC
6	Durante las situaciones de emergencia el brigadista pondrá en práctica los simulacros desarrollados con el personal, a fin de salvaguardar la integridad física del personal	CO/CAODPE/AUX. DIURNO/NOCTURNO
7	Comunicarse, a la brevedad posible, con los Bomberos, Defensa Civil y la PNP.	Personal ODPE/ORC
8	Acciones posteriores Evaluación de daños. Rescatar la documentación y/o material electoral. Reunir al personal y reforzar las medidas de seguridad. Cargar los extintores empleados.	JODPE/ Gestor ORC

4.8. Acciones a implementar frente a un Sismo o Terremoto

N°	Descripción de la tarea	Responsable
1	Brindar información y capacitación a los JODPE sobre acciones a tomar frente a un sismo o terremoto	OSDN
2	Coordinar los simulacros de sismo o terremoto	OSDN
3	Ejecutar los simulacros de sismo o terremoto, dispuesto por la entidad competente y/o pro la OSDN, según el anexo 2	JODPE
4	Identificar y señalizar las zonas de seguridad internas y externas en la sede de la ODPE u ORC.	CAODPE/CO ODPE/Gestor ORC
5	Identificar las rutas de evacuación y mantenerlas libres	CAODPE/CO/ Gestor ORC
6	Preparar la mochila de emergencia la cual deberá contener	JODPE/ Gestor

N°	Descripción de la tarea	Responsable
	preferentemente: botiquín de primeros auxilios, linterna portátil, radio a pilas portátil y agua.	ORC
7	En caso de ocurrencia: ▪ Adoptar inmediatamente, las medidas de seguridad para la protección, y evacuación del personal. ▪ Activar las brigadas de emergencia.	JODPE/ Gestor ORC
8	Reunir al personal y revisar las medidas de seguridad.	JODPE/ Gestor ORC
9	El brigadista evalúa daños humanos y materiales y determina quienes requieren asistencia médica y si el local es aún habitable	JODPE/ Gestor ORC
10	Informar de inmediato, usando el medio más idóneo, a la GOECOR	JODPE/ Gestor ORC
11	Elaborar el informe correspondiente y remitirlo a la GOECOR	JODPE/ Gestor ORC

5. EVALUACIÓN DE ACCIONES IMPLEMENTADAS

5.1. Informes de acciones implementadas

N°	Descripción de la tarea	Responsable
1	Elaborar los informes correspondientes a cada una de las acciones de seguridad tomadas y descritas en este documento, así como incluir en el informe la lista de verificación indicada en el anexo 1 y remitirla a través del SGD a la GOECOR.	JODPE/Gestor ORC
2	Remitir el Informe de las ODPE y/o ORC a la OSDN para la evaluación y el análisis respectivo.	GOECOR OSDN
3	Recibir de la OSDN, el informe de evaluación y análisis en relación al informe remitido por la ODPE/ORC de las acciones de seguridad tomadas.	GOECOR

	OTROS DOCUMENTOS	Código:	OD01- OSDN/SP
		Versión:	01
	ACCIONES A IMPLEMENTAR PARA PREVENIR Y/O ATENDER CONTINGENCIAS POR EMERGENCIAS Y DESASTRES EN LAS SEDES DE LA ODPE Y LAS ORC	Página:	9 de 14

6. ANEXOS

6.1. Anexo 1:

Formato: Ficha de verificaciones de las acciones preventivas realizadas en la ODPE y las ORC.

LISTA DE VERIFICACIÓN		
Nombre de la Persona que registra:		
ACCIONES PREVENTIVAS	**Registrar (√) si es conforme y (X) si no es conforme.**	**OBSERVACIONES**
I. EN CASO DE INUNDACION		
a) Cuentan con buen estado las tuberías de agua y desagüe de los ambientes de la ODPE o de las ORC.		
b) Se encuentran las señaléticas de las zonas de seguridad internas y externas de la ODPE o de las ORC.		
c) Existen designados brigadistas de emergencia.		
II. EN CASO DE CORTE DE FLUIDO ELÉCTRICO		
a) Verificar las instalaciones eléctricas del local, conexiones e interruptores y tomacorriente.		
III. EN CASO DE OCURRENCIA DE EMERGENCIA DE SALUD CON EL PERSONAL		
a) Cuenta con el listado de teléfonos de emergencia y direcciones de hospitales, puestos de salud, entre otros publicado en lugares visibles.		
b) Cuentan con Botiquín de primeros auxilios.		
IV. INCENDIO		
a) Los materiales inflamables están en lugar seguro.		
b) Cuentan con extintores y cuantos son		
c) Existen señaléticas de: No fumar, peligro electricidad, inflamable entre otros.		
d) Existen el listado de los teléfonos de emergencia y direcciones de los bomberos, defensa civil, PNP, centros hospitalarias entre otros.		

	OTROS DOCUMENTOS	Código:	OD01- OSDN/SP
		Versión:	01
	ACCIONES A IMPLEMENTAR PARA PREVENIR Y/O ATENDER CONTINGENCIAS POR EMERGENCIAS Y DESASTRES EN LAS SEDES DE LA ODPE Y LAS ORC	Página:	10 de 14

6.2. Anexo N°2

Guía Para La Realización De Un Simulacro de Evacuación por Sismo e Incendio.

Previo al Simulacro

Actividad	Responsable
a) Fijar la fecha y la hora del simulacro (informado previamente por la OSDN).	Gestor de la ORC /JODPE
b) Informar a todo el personal de la realización del simulacro. Publicar en periódicos murales, etc.	Gestor de la ORC /JODPE
c) Verificación previa de las condiciones adecuadas de las instalaciones, señalización e iluminación de emergencia de los recorridos de evacuación y contar con extintores, arena, mantas contra fuego.	Gestor de la ORC /JODPE
d) Designar el lugar y la persona que inicia el simulacro.	Gestor de la ORC /JODPE
e) Dar instrucciones a los trabajadores de la ODPE u ORC.	Gestor de la ORC /JODPE
f) Dar la alarma de aviso para el simulacro.	Gestor de la ORC /JODPE

El Mismo día del Simulacro (Rol)

El Brigadista:

a) Previsión de posibles accidentes durante el simulacro (por ejemplo, donde se pueden golpear o caer) y disponer del botiquín de Primeros Auxilios.
b) Realización del simulacro:
   Al oír la alarma, el personal evacúa y se dirige a la zona segura, considerando la ubicación del amago de fuego.
c) Información a los empleados del resultado del simulacro y conclusiones del mismo.
d) Tras la finalización del simulacro, redactar el informe de la actuación de los participantes y las conclusiones y propuestas de mejora deducidas del mismo, según Anexo 3.

	OTROS DOCUMENTOS	Código:	OD01- OSDN/SP
		Versión:	01
	ACCIONES A IMPLEMENTAR PARA PREVENIR Y/O ATENDER CONTINGENCIAS POR EMERGENCIAS Y DESASTRES EN LAS SEDES DE LA ODPE Y LAS ORC	Página:	11 de 14

6.3. Anexo N° 3

Modelo de Informe de Simulacro

INFORME N°...

SIMULACRO DE EMERGENCIA POR INCENDIO /SISMO

DESARROLLO

En la ORC/ODPE:.....ubicada en .....

Se produce un supuesto .....incendio / simulacro de sismo el dia ..... y hora ..... en el área de ..... cuyo personal asignado por el ORC/JODPE o responsable de la ORC/ODPE ..... activan la alarma.

El brigadista.....avisa a sus compañeros indicando que se requiere la evacuación de todo el local como medida de seguridad para controlar el amago de fuego usando el extintor.

OBJETIVOS

Los Objetivos del Simulacro fueron:

a) Comprobar la idoneidad del punto de reunión o zona segura en el exterior del local.
b) Comprobar el tiempo máximo de concentración del personal en el Punto de Reunión.
c) Que todo el personal conozca las vías de evacuación.
d) Conocer las posibles dificultades de salida de cada uno de los recorridos.

(Indicar que se observa durante el simulacro sobre la reacción de los colaboradores y personas que se encuentran en el local)

.....
.....
.....

RESULTADOS

a) Colocar el Tiempo (minutos) (Medir el tiempo en el que se produce la salida de la primera persona y de la última)
b) Número de participantes.
c) Número de Brigadistas, titulares y suplentes (si los hay).

	OTROS DOCUMENTOS	Código:	OD01- OSDN/SP
		Versión:	01
	ACCIONES A IMPLEMENTAR PARA PREVENIR Y/O ATENDER CONTINGENCIAS POR EMERGENCIAS Y DESASTRES EN LAS SEDES DE LA ODPE Y LAS ORC	Página:	12 de 14

7. CUADRO DE CONTROL DE CAMBIOS

Versión anterior	Fecha de aprobación	Sección / Ítem	Categoría N: nuevo M: Modificado E: Eliminado	Principales cambios realizados con respecto a la versión anterior
00	25/06/2014	TITULO	M	Se modifica de "Contingencias en las Sedes de la ODPE, Oficinas Distritales y las ORC" por "Acciones a implementar para prevenir y/o atender Contingencias por Emergencias y Desastres en las Sedes de la ODPE y las ORC".
00	25/06/2014	Base Legal	N	D.S. N° 002-2018-PCM: Nuevo Reglamento de Inspecciones Técnicas de Seguridad en Edificaciones.
00	25/06/2014	Base Normativa	E	▪ Plan General de Conservación Documental de la ONPE. ▪ Resolución Jefatural N° 159-97-AGN/J. ▪ D.S. N° 001-A-2004-DE-SG.
00	25/06/2014	Abreviaturas	N	Se agregó una tabla de abreviaturas con sus respectivos términos.
00	25/06/2014	4.1 / Aspectos Generales (ODPE)	N	Se agregó este ítem con la finalidad de saber las actividades generales a realizarse en una contingencia.
00	25/06/2014	1.1	M	Se modificó a "Acciones a implementar frente a casos de Inundación".
00	25/06/2014	1.1 / Acciones Preventivas	N	▪ Se incorpora en el ítem "A" el registro en el formato del anexo 1. ▪ Se incluye la identificación y señalización según INDECI del ítem "C" en el ítem 4.1. ▪ Se incluye la estructura de Organización de Brigadas en el ítem 4.1.
00	25/06/2014	1.1 / En Caso de Ocurrencia	E	Actividad de instalar ventiladores para el secado de documentación del material electoral.
00	25/06/2014	1.1 / Acciones Posteriores	M	Del ítem "a" se modifica "Estar dispuesto a proporcionar..." por "Coordinar los primeros auxilios...".
00	25/06/2014	1.1 / Acciones Posteriores	E	Actividades del ítem "E" relativos a: ▪ El cuidado especial de su manipulación. ▪ Especificaciones del secado manual. ▪ Uso de hilos de pesca para colgar parcialmente las hojas.

	OTROS DOCUMENTOS	Código:	OD01- OSDN/SP
		Versión:	01
	ACCIONES A IMPLEMENTAR PARA PREVENIR Y/O ATENDER CONTINGENCIAS POR EMERGENCIAS Y DESASTRES EN LAS SEDES DE LA ODPE Y LAS ORC	Página:	13 de 14

Versión anterior	Fecha de aprobación	Sección / Ítem	Categoría N: nuevo M: Modificado E: Eliminado	Principales cambios realizados con respecto a la versión anterior
00	25/06/2014	1.2	M	Se modificó a "Acciones a implementar frente a casos de problemas o cortes del fluido eléctrico".
00	25/06/2014	1.2 / Acciones Preventivas	N	▪ Se incluye que la revisión debe ser registrada según Anexo 1. ▪ Se incluye que la carga utilizada debe estar de acuerdo al plano de distribución eléctrica. ▪ Se especifica que el alquiler de extintores deben ser de PQS y CO2.
00	25/06/2014	1.2 / Acciones Preventivas	E	La actividad de que los empalmes estén debidamente asegurados.
00	25/06/2014	1.2 / Acciones Posteriores	E	Se eliminó los ítem c y d.
00	25/06/2014	1.3	M	Se modificó a "Acciones a implementar frente a casos de emergencias de Salud con el personal"
00	25/06/2014	1.3 / En Caso de Ocurrencia	E	Se eliminó la actividad del ítem "g".
00	25/06/2014	1.4	M	Se modificó a "Acciones a implementar frente a casos de ocurrencia de actos delictivos".
00	25/06/2014	1.4.1 / Acciones Preventivas	E	La actividad del ítem "c".
00	25/06/2014	1.4.1 / Acciones de Ocurrencia	E	Se eliminó la actividad b, c, d.
00	25/06/2014	1.4.1 / Acciones Posteriores	E	La actividad del ítem b, c, d, e, f y g.
00	25/06/2014	1.4.2	E	Las actividades en caso de Intrusión tanto preventivas, en caso de ocurrencia y posteriores.
00	25/06/2014	1.4.3	M	Se modificó a "Acciones a implementar frente a casos de Sabotaje a la sede, o a los bienes muebles".
00	25/06/2014	1.4.3 / Acciones Preventivas	E	La actividad del ítem "a".
00	25/06/2014	1.4.3 / Acciones	E	La actividad del ítem "e".

	OTROS DOCUMENTOS	Código:	OD01- OSDN/SP
		Versión:	01
	ACCIONES A IMPLEMENTAR PARA PREVENIR Y/O ATENDER CONTINGENCIAS POR EMERGENCIAS Y DESASTRES EN LAS SEDES DE LA ODPE Y LAS ORC	Página:	14 de 14

Versión anterior	Fecha de aprobación	Sección / Ítem	Categoría N: nuevo M: Modificado E: Eliminado	Principales cambios realizados con respecto a la versión anterior
		Posteriores		
00	25/06/2014	1.4.4	M	Se modificó a "Acciones a implementar frente a casos de Incendio".
00	25/06/2014	1.4.4 / Acciones Preventivas	E	La actividad del ítem "j".
00	25/06/2014	1.4.4 / Acciones Preventivas – "m"	N	Se incluye la realización de simulacros según lo dispuesto en el Anexo 2 del presente documento.
00	25/06/2014	1.4.4 / Acciones Posteriores	E	La actividad del ítem "d".
00	25/06/2014	4.8	N	Se agregó el ítem "Acciones a implementar frente a un Sismo o Terremoto".
00	25/06/2014	5 / Evaluación de acciones implementadas	N	Se agregó un ítem sobre la Evaluación de Acciones Implementadas.
00	25/06/2014	5 ANEXOS	N	Anexo 1, 2 y 3.
00	25/06/2014	Varios	N	Se incluye actividades de Desastres Naturales.

ANEXO K OD02-OSDN/SP OCURRENCIAS DE CONMOCIÓN SOCIAL

	OTROS DOCUMENTOS	Código:	OD02-OSDN/SP
ONPE		Versión:	00
	OCURRENCIA DE CONMOCIÓN SOCIAL	Página:	1 de 2

Elaborado por:	Revisado por:	Aprobado por:
Patricia Janette Vargas Rodríguez Subgerente de Patrimonio Documental 16 JUN. 2014	Edilberto Terry Ramos Gerente de la Oficina de Seguridad y Defensa Nacional (e) 25 JUN. 2014 Amparo Ortega Campana Gerente de Gestión de la Calidad (e) 19 JUN. 2014	Edilberto Terry Ramos Gerente de la Oficina de Seguridad y Defensa Nacional (e) 25 JUN. 2014

En caso de ocurrencia de situaciones de conmoción social (paros, huelgas, marchas de protesta) en la circunscripción de la ODPE y/o Oficinas Distritales, el responsable o el JODPE debe de ejecutar las siguientes acciones:

Acciones Preventivas	En caso de Ocurrencia	Acciones Posteriores
a. Estar informado de las asambleas, reuniones y acuerdos de gremios y otros actores sociales. b. Recabar información sobre la posible realización de marchas, paros o acciones de protesta, de la PNP o de los gobernadores o tenientes gobernadores, en caso que existan en la jurisdicción. c. Recabar información de los actores políticos y sociales (sacerdotes, médicos, enfermeras, profesores, etc.). d. De ser posible, conocer el itinerario del personal de la sede de la ODPE o de la Oficina Distrital, que está realizando actividades propias del proceso electoral. e. Organizar al personal de modo tal que las labores se realicen con un mínimo de dos personas. f. Evitar el traslado innecesario de material de capacitación, durante el desarrollo de	a. Adoptar medidas de seguridad para la protección del local y evacuación del personal; si el paro, huelga o marcha de protesta se torna violenta, adoptar las siguiente medidas: - Cerrar inmediatamente las puertas del local de la ODPE u oficina distrital. - No salir del local de la ODPE u oficina distrital. b. Si la aglomeración de personas se está llevando a cabo en un lugar cercano a la sede de la ODPE o a las oficinas distritales: - Disponer que únicamente ingresen al o los locales, personas debidamente identificadas. - Evaluar la pertinencia de atender a puertas cerradas. - Evitar acercarse a la multitud. c. Disponer que el personal no participe bajo ninguna circunstancia en asambleas o reuniones	a. Evaluar el impacto de los hechos en la vida de la comunidad y para el o los procesos electorales y sus posibles consecuencias. b. Informar diariamente a la GOECOR desde una semana antes del día del proceso electoral.

	OTROS DOCUMENTOS	Código:	OD02-OSDN/SP
		Versión:	00
	OCURRENCIA DE CONMOCIÓN SOCIAL	Página:	2 de 2

Acciones Preventivas	En caso de Ocurrencia	Acciones Posteriores
dichas actividades. g. Intercambiar información con los responsables de los otros organismos electorales, respecto a la situación socio política de la zona.	organizadas por actores sociales. d. Si se encuentra fuera del local de la ODPE u oficina distrital, refugiarse en un lugar seguro. e. Reportar los hechos a la GOECOR por medio de correo electrónico o llamada telefónica, la misma que a su vez deberá alcanzar dicha información a la OSDN.	

Anexo "L" DI04-GGC/GC Lineamientos de Seguridad de la Información

ONPE
OFICINA NACIONAL DE PROCESOS ELECTORALES

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Elaborado por:	Revisado por:
Verónica Ordóñez Dávila Oficial de Seguridad de la Información 15 MAR 2017	Patricia Janette Vargas Rodriguez Secretaria General (e) 15 MAR 2017 Gilbert Fernando Vallejos Arrieta Gerente de la Gerencia General 15 MAR 2017 Jaime Enrique Molina Vilchez Gerente de Gestión de la Calidad 15 MAR 2017 Erik Ulises Bazán Flores Gerente de Información y Tecnología Electoral (e) 15 MAR 2017 Adelmo Cancino Cancino Gerente de Gestión Electoral 15 MAR 2017 Mary del Rosario Jessen Vigil Gerente de Planeamiento y Presupuesto 15 MAR 2017 Henry Josue Orna Robladillo Gerente de Organización de Locales y Coordinación Regional (e) 15 MAR 2017 Fernando Lopez Villafuerte Gerente de Supervisión de Fondos Partidarios (e) 15 MAR 2017 Heidi Veronica Landa Camayo Gerente de Información y Educación Electoral (e) 15 MAR 2017 Sandra Lucy Portocarrero Peñaflel Gerente de Asesoría Jurídica 15 MAR 2017 Fernando López Villafuerte Gerente de la Oficina de Seguridad y Defensa Nacional 15 MAR 2017 Sessy Betsy Alejos Sevillano De Escudero Gerente Corporativo de Potencial Humano 15 MAR 2017 Gustavo Elias Dominguez Lopez Gerente de Administración 15 MAR 2017 Paola Saverden Cabezudo Gerente de Comunicaciones y Relaciones Corporativas (e) 15 MAR 2017
Código: DI04-GGC/GC **Versión: 00**	

ONPE	DIRECTIVA	Código:	DI04-GGC/GC
		Versión:	00
	LINEAMIENTOS DE SEGURIDAD DE LA INFORMACION	Página:	1 de 26

ÍNDICE

ONPE	DIRECTIVA	Código:	DI04-GGC/GC
		Versión:	00
	LINEAMIENTOS DE SEGURIDAD DE LA INFORMACION	Página:	2 de 26

1. OBJETIVO

Establecer las normas relacionadas a la seguridad de la información a fin de asegurar y mantener su confidencialidad, integridad y disponibilidad.

2. ALCANCE

Es de aplicación para todo el personal de la institución contratado bajo cualquier modalidad, proveedores de servicios y terceros.

3. BASE NORMATIVA

3.1. Resolución Ministerial Nº 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

3.2. Resolución Ministerial Nº 246-2007-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas entidades integrantes del Sistema nacional de Informática.

3.3. Resolución Directoral Nº 001-2013-JUS/DGPDP que aprueba los formularios para la inscripción de bancos de datos personales de administración privada por persona natural, de administración privada por persona jurídica y de administración pública.

3.4. Ley N° 27806 – Ley de Transparencia y Acceso a la Información Pública y su reglamento.

3.5. Ley N° 29733 – Ley de Protección de Datos Personales, su reglamento y su directiva.

3.6. Ley N° 27269 – Ley de Firmas y Certificados Digitales y su reglamento.

3.7. Ley 27815 – Ley del Código de Ética de la Función Pública.

3.8. Decreto Legislativo N° 681 - "Dictan normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la elaborada en forma convencional cuanto la producida por procedimientos informáticos en computadoras" y su reglamento.

3.9. Norma Técnica Peruana NTP 392.030-2:2015 Microformas. Requisitos para las organizaciones que operan sistemas de producción de microformas. Parte 2: Medios de Archivo Electrónico.

3.10. Directiva del Instituto Nacional de Estadística e Informática "Normas técnicas para el almacenamiento y respaldo de la información procesada las Entidades de la Administración Pública".

3.11. Reglamento de Organización y Funciones de la Oficina Nacional de Procesos Electorales.

3.12. Reglamento Interno de Trabajo de la Oficina Nacional de Procesos Electorales.

3.13. Manual de Organización y Funciones de la Oficina Nacional de Procesos Electorales.

Nota: Los documentos mencionados son los vigentes incluyendo sus modificatorias.

4. REFERENCIAS

4.1. Política de Protección de Datos Personales de la Oficina Nacional de Procesos Electorales.

4.2. Política de Seguridad de la Información de la Oficina Nacional de Procesos Electorales.
4.3. Objetivos de Seguridad de la Información de la Oficina Nacional de Procesos Electorales.

Nota: Los documentos mencionados son los vigentes incluyendo sus modificatorias.

5. DEFINICIONES Y ABREVIATURAS

5.1. Definiciones

5.1.1. Activos de información: Recursos humanos, tecnológicos, administrativos, etc. que participan en el tratamiento de la información.

5.1.2. Cifrado: Es una forma de tratamiento que permite que la información electrónica sea leíble y modificada solo por las personas autorizadas, asegurando así su confidencialidad e integridad respectivamente.

5.1.3. Comité de Gestión de Seguridad de la Información: Es el comité que tiene por función gestionar la seguridad de la información en la institución. Se conforma por Resolución Jefatural.

5.1.4. Confidencialidad: Cualidad de prevenir la divulgación de la información a personas o sistemas no autorizados.

5.1.5. Datos personales: Son aquellos que identifican directa o indirectamente a una persona natural (titular de los datos): nombre, fecha de nacimiento, dirección de domicilio y de correo electrónico; números del DNI, RUC, teléfono, celular, seguro social y placa de vehículo; imagen; firma manuscrita y electrónica; y otros datos no sensibles establecidos en los formularios aprobados con Resolución Directoral Nº 001-2013-JUS/DGPDP (08 de mayo de 2013).

5.1.6. Datos personales sensibles: Son aquellos que pueden ser objeto de tratamiento con el consentimiento expreso y por escrito de la persona natural (titular de los datos) y, por lo tanto, requieren especial protección: datos biométricos (huella dactilar o digital, retina, iris); datos de origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; datos relacionados a la salud o a la vida sexual; y hechos o circunstancias de la vida afectiva o familiar.

5.1.7. Disponibilidad: Característica que determina la accesibilidad de la información a personas, procesos o sistemas en el lugar y momento oportunos.

5.1.8. Dispositivos móviles institucionales: Aparatos electrónicos como computadoras portátiles, *tablets*, celulares o *smartphones*, acceso portable a datos (PDA), dispositivos de almacenamiento USB u otros que permitan el tratamiento de la información durante su desplazamiento y uso en ambientes no controlados por la institución.

5.1.9. Encargado del banco de datos personales: Personal designado, mediante resolución jefatural, por la Jefatura Nacional como responsable de la seguridad de los bancos de datos personales que administra la institución en el ámbito de la Ley de Protección de Datos Personales.

5.1.10. Gestión de riesgos: Consiste en la identificación, análisis y evaluación de riesgos, así como la planificación, implementación y su correspondiente seguimiento de las acciones de tratamiento del riesgo.

5.1.11. Integridad: Propiedad que busca garantizar una información exacta y libre de errores, la misma que puede ser modificada bajo autorización.

5.1.12. Interesados: Personas u organizaciones que tienen una responsabilidad, necesidad, expectativa, o cualquier otro interés que involucra a la institución. Pueden afectar o ser afectados por alguna decisión o actividad. Ejemplo: personal; proveedores; socios por convenio interinstitucional; entidades observadoras, reguladoras, supervisoras y fiscalizadoras; y clientes.

5.1.13. Líder usuario: Personal responsable de definir y aceptar el cumplimiento de los requerimientos y requisitos del producto software. Es designado por el órgano o unidad orgánica solicitante del producto software.

5.1.14. Medios de almacenamiento removibles: Son aquellos dispositivos que se insertan a los conectores externos de los equipos informáticos para almacenar información, tales como memoria USB, disco duro externo o tarjetas de memoria.

5.1.15. Controles criptográficos: Son aquellos controles que protegen la confidencialidad e integridad de la información electrónica durante su procesamiento, almacenamiento o transmisión y que comprueban la identidad de quienes acceden a esta.

5.1.16. Oficial de Seguridad de la Información: Personal designado mediante, resolución jefatural, por la Jefatura Nacional, que tiene la responsabilidad de supervisar la implementación de la Política y objetivos de Seguridad de la Información de la institución, alineando los controles y recursos de acuerdo a la gestión de los riesgos.

5.1.17. Oficial de Seguridad EREP: Personal designado, mediante resolución gerencial, por la Gerencia de Organización Electoral y Coordinación Regional para coordinar la seguridad de la información que administra la institución como Entidad de Registro para el Estado Peruano en el ámbito de la Ley de Firmas y Certificados Digitales.

5.1.18. Oficial de Privacidad EREP: Personal designado, mediante resolución gerencial, por la Gerencia de Organización Electoral y Coordinación Regional para coordinar la protección de los datos personales que administra la institución como Entidad de Registro para el Estado Peruano en el ámbito de la Ley de Firmas y Certificados Digitales.

5.1.19. PeCERT: Grupo de trabajo permanente, denominado Coordinadora de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública del Perú, en el ámbito de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros. Se encarga de coordinar con las instituciones públicas para afrontar diversas amenazas de las redes teleinformáticas a los que está expuesta la información que producen o administran, con el fin de proveer a la Nación de una postura segura en el ámbito de la seguridad informática.

5.1.20. Propietario de activo: Órgano de la ONPE responsable, determinado en un inventario de activos de información, que tiene la responsabilidad y autoridad, dentro del alcance de sus competencias, de asegurar el buen uso, funcionamiento y protección del activo de información mientras está a su cargo a fin de que cumpla con los objetivos para los cuales se le adquirió.

5.1.21. Propietario de riesgo: Órgano de la ONPE que se ve afectado por el riesgo y tiene responsabilidad y autoridad para gestionarlo.

5.1.22. Redes inalámbricas públicas: Son aquellas redes inalámbricas ubicadas en lugares públicos tales como restaurantes, centros comerciales, buses, hoteles, etc. en donde cualquier dispositivo móvil, institucional o no, puede conectarse a ellas.

5.1.23. Responsable de Seguridad Tecnológica: Personal designado, mediante resolución gerencial, por la Gerencia de Informática y Tecnología Electoral, que tiene como propósito coordinar las acciones para prevenir o mitigar los riesgos de origen tecnológico.

5.1.24. Responsable del Sistema de Gestión del órgano: Personal designado, mediante memorando, por el Órgano que tiene como propósito liderar aspectos de gestión de la calidad, seguridad de la información y otros en el ámbito del órgano al cual pertenece.

5.1.25. Riesgo: Probabilidad de que un evento, suceso o acontecimiento perjudicial (no deseado) o beneficioso (deseado), degrade o aumente el grado de la confidencialidad, integridad y disponibilidad de la información que maneja un determinado proceso o proyecto.

5.1.26. Sistema de información: Es todo sistema soportado por una infraestructura tecnológica informática.

5.1.27. Tratamiento de información: Es la acción, automatizada o no, de crear, elaborar, recopilar, registrar, almacenar, cifrar, consultar, usar, organizar, modificar, copiar, extraer, transferir, transmitir, distribuir, bloquear, procesar, conservar, eliminar, suprimir o destruir la información.

5.1.28. Usuarios: Personal de la institución contratado bajo cualquier modalidad, proveedores de servicios y terceros que tienen acceso a la información a través de medios convencionales u automatizados.

5.2. Abreviaturas

5.2.1.	APDP	: Autoridad Nacional de Protección de Datos Personales.
5.2.2.	AAC	: Autoridad Administrativa Competente.
5.2.3.	CGSI	: Comité de Gestión de Seguridad de la Información.
5.2.4.	EC	: Entidad de Certificación
5.2.5.	EREP	: Entidad de Registro del Estado Peruano.
5.2.6.	GCPH	: Gerencia Corporativa de Potencial Humano.
5.2.7.	GG	: Gerencia General.
5.2.8.	GGC	: Gerencia de Gestión de la Calidad.
5.2.9.	GIEE	: Gerencia de Información y Educación Electoral.
5.2.10.	GITE	: Gerencia de Informática y Tecnología Electoral.
5.2.11.	INDECOPI	: Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.
5.2.12.	JN	: Jefatura Nacional.
5.2.13.	LPDP	: Ley de Protección de Datos Personales.
5.2.14.	ODPE	: Oficina Descentralizada de Procesos Electorales.
5.2.15.	ONPE	: Oficina Nacional de Procesos Electorales.
5.2.16.	OSDN	: Oficina de Seguridad y Defensa Nacional.
5.2.17.	OSI	: Oficial de Seguridad de la Información.
5.2.18.	SG	: Secretaría General.
5.2.19.	SGSI	: Sistema de Gestión de Seguridad de la Información.
5.2.20.	TI	: Tecnología de la Información.

6. NORMAS GENERALES

6.1. Organización de la seguridad de la información

6.1.1. Organización interna

La ONPE ha establecido los siguientes roles y funciones para la gestión de la seguridad de la información:

A. Comité de Gestión de Seguridad de la Información (CGSI)

a) Revisar las políticas, objetivos, planes, normas, responsabilidades y propuestas de mejora que reciba, asociados a la seguridad de la información, y de considerarlo pertinente, elevarlas a JN para su consideración y posterior aprobación, así como evaluar su cumplimiento.
b) Definir las estrategias de la institución respecto a la implementación de normas del Estado Peruano y estándares internacionales referidos a la seguridad de la información.
c) Revisar la Política de Seguridad de la Información una vez al año o cuando se realice alguna modificación significativa que impacte en la institución; y formular, a través del OSI, las modificaciones que correspondan para su aprobación por la JN.
d) Asegurar la comunicación a los usuarios sobre la Política y Objetivos de Seguridad de la Información, así como de los Lineamientos de Seguridad de la Información, la importancia de su cumplimiento; así como, sus responsabilidades de acuerdo a la Ley.

e) Garantizar la implementación, operación, revisión, mantenimiento y mejora del SGSI; y evaluar por lo menos una vez al año sus resultados.
f) Cumplir con alguna otra función establecida en el ordenamiento jurídico del Estado Peruano en materia de seguridad de la información.

B. Propietario de Riesgo

a) Gestionar los riesgos de seguridad de la información dentro del alcance de sus competencias.

C. Oficial de Seguridad de la Información (OSI)

a) Proponer a los demás miembros del CGSI las políticas, objetivos, lineamientos, planes, roles y funciones necesarias para la ~~administración~~ gestión técnica y efectiva de la seguridad de la información.
b) Coordinar la ejecución de la evaluación de riesgos de seguridad de la información y de sus resultados.
c) Coordinar con el Oficial de Seguridad de la EREP y los Responsables del Sistema de Gestión y de Seguridad Tecnológica, la adecuada implementación de las políticas, objetivos, planes y controles de seguridad de la información que les corresponda.
d) Verificar que las ejecuciones de las pruebas hayan cumplido con los procedimientos relacionados con la continuidad de la seguridad de la información.
e) Identificar las necesidades de capacitación, difusión y sensibilización en seguridad de la información.

D. Oficial de Seguridad de la EREP

a) Velar por la estricta observancia de la política, objetivos y lineamientos de Seguridad de la Información de la institución dentro del alcance de la EREP-ONPE.
b) Cuidar que los procesos y procedimientos relacionados a la firma digital, se realicen en el marco de la Infraestructura Oficial de Firma Electrónica, garantizando el no repudio de los documentos electrónicos generados por la EREP-ONPE.
c) Proponer las acciones necesarias para dar cumplimiento a la política, objetivos y lineamientos de Seguridad de la Información que se encuentren dentro del alcance de la EREP-ONPE.
d) Asegurar la implementación de controles de seguridad de la información para los procesos a cargo de la EREP-ONPE.
e) Revisar permanentemente la política, objetivos y lineamientos de Seguridad de la Información dentro del alcance de la EREP-ONPE, proponiendo de ser el caso su actualización.
f) Promover la adopción de buenas prácticas en materia de seguridad de la información.
g) Identificar las necesidades de capacitación y sensibilización para una adecuada protección de la seguridad de la información, dentro del marco de los servicios de la EREP-ONPE.
h) Adoptar las medidas correctivas en caso se identifique algún tipo de vulneración real o potencial de la seguridad de la información.

i) Gestionar los riesgos y dar respuesta ante incidentes en los procesos a cargo de la EREP-ONPE.
j) Determinar y analizar los requerimientos necesarios para la recuperación en caso de desastres.

E. Responsable de Seguridad Tecnológica

a) Administrar los procesos de seguridad tecnológica.
b) Proponer guías, normas o estándares de seguridad para el diseño de las soluciones tecnológicas que se implementen.
c) Elaborar los planes de seguridad tecnológica y de contingencia.
d) Ejecutar charlas de sensibilización al personal sobre aspectos de seguridad tecnológica.
e) Participar en la implantación del programa de seguridad de la información de acuerdo a los lineamientos establecidos por el CGSI.
f) Identificar y gestionar los riesgos e incidentes de seguridad tecnológica.
g) Coordinar la ejecución del análisis de vulnerabilidades para los servicios tecnológicos y asegurar su tratamiento.
h) Asumir las funciones del OSI ante su ausencia.

F. Responsables del Sistema de Gestión del órgano

a) Coordinar con los involucrados del órgano al cual pertenecen respecto a la implementación del cumplimiento de la Política, objetivos y lineamientos de Seguridad de la Información y de las acciones de tratamiento de riesgos; a su vez, efectuar el seguimiento respectivo.
b) Proponer controles de seguridad durante la elaboración o actualización de las directivas, procedimientos e instructivos para mejorar los niveles de seguridad de la información existentes.
c) Apoyar en la gestión de los riesgos de seguridad de la información.
d) Respaldar durante las auditorías internas de seguridad de la información al personal auditado del órgano al cual pertenecen.
e) Coordinar con los involucrados del órgano la solución de incidentes de seguridad de la información dentro del alcance de sus competencias.
f) Capacitar y sensibilizar en temas de seguridad de la información al personal involucrado del órgano al cual pertenecen.
g) Difundir la Política, objetivos y lineamientos de Seguridad de la Información.
h) Durante la creación o actualización de procedimientos e instructivos, asegurar la segregación de tareas del personal involucrado para reducir los riesgos de modificaciones no autorizadas, así como del uso indebido de los activos de información.

G. Encargado del Banco de Datos Personales

a) Asegurar la implementación de los controles de seguridad de los datos personales según normas emitidas por la APDP.

H. Oficial de Privacidad de la EREP

a) Velar por la estricta observancia de la Política de Protección de Datos Personales de la ONPE dentro del ámbito de la EREP-ONPE.

b) Proponer la adopción de buenas prácticas en materia de protección de datos personales tratados por la EREP-ONPE.
c) Identificar las necesidades de capacitación y sensibilización para una adecuada protección de los datos personales, dentro del marco de los servicios de la EREP-ONPE.
d) Implementar las medidas correctivas en caso se identifique algún tipo de vulneración real o potencial, relacionado al tratamiento de los datos personales por la EREP-ONPE.
e) Coordinar permanentemente con el Encargado del Banco de Datos Personales de la ONPE las acciones o controles a implementar relacionados al tratamiento de los datos personales.
f) Reportar, a solicitud del Encargado del Banco de Datos Personales, las incidencias relacionadas al tratamiento de datos personales, así como el progreso de las acciones y controles a implementar por la EREP ONPE.

I. Todo el personal en general

a) Cumplir y hacer cumplir al personal a su cargo, a los proveedores de servicios y a los terceros con quienes coordine, las políticas, objetivos y lineamientos de seguridad de la información que apliquen de la presente directiva.
b) Participar en la implementación de la política, objetivos y lineamientos de seguridad de la información, así como de las acciones de tratamiento de riesgos y acciones correctivas de acuerdo al alcance de sus competencias.
c) Reportar los eventos, incidentes y debilidades de seguridad de la información de acuerdo a los procedimientos establecidos por la institución.

6.1.2. Dispositivos móviles institucionales

La GITE debe:

a) Configurar en los dispositivos móviles institucionales el tiempo de inactividad para el bloqueo automático del mismo; así como, algún método de seguridad para su desbloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz).
b) Implementar controles criptográficos en los dispositivos móviles institucionales a solicitud de los usuarios cuando estos almacenen información laboral que no sea de carácter público.
c) Con respecto a los dispositivos móviles institucionales empleados en las Soluciones Tecnológicas de Voto Electrónico, asegurar que se implementen todos los controles de seguridad necesarios y adecuados para cada modalidad de votación electrónica con la finalidad de asegurar la confidencialidad, integridad y disponibilidad de la información.

Los usuarios deben:

d) Evitar el uso de los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias, para evitar pérdida o robo de estos.

e) Evitar la modificación de las configuraciones de seguridad de los dispositivos móviles institucionales, ni la desinstalación del software provisto en ellos. De requerirlo, deben solicitárselas a la GITE.

f) Evitar el uso de redes inalámbricas públicas para prevenir riesgos de seguridad a la información almacenada en el dispositivo móvil institucional.

g) Realizar el respaldo de su información laboral almacenada en su dispositivo móvil institucional.

6.1.3. Teletrabajo

a) Solo los usuarios que administran sistemas de información están permitidos a ingresar a estos, desde fuera de las instalaciones de la institución y mediante canales de comunicación seguros (encriptados) previa autenticación, para brindar soporte ante la pérdida o degradación del servicio, contando con la autorización de su propietario.

b) Los usuarios solo deben acceder desde fuera de las instalaciones de la institución a los sistemas de información previa autorización del responsable del órgano al cual pertenece.

6.2. Seguridad relacionada con los Recursos Humanos

La ONPE debe promover una cultura en seguridad de la información, de tal manera que las acciones del personal no conduzcan a poner en riesgo a la confidencialidad, integridad y disponibilidad de la información.

6.2.1. Antes del empleo

a) La GCPH debe comprobar el cumplimiento de los requisitos del personal que ingresa a laborar en la institución, de acuerdo a las leyes y regulaciones vigentes, independientemente de su modalidad de contrato. Como mínimo, debe verificar, de acuerdo a los procedimientos establecidos, lo siguiente:

a.1) Validez del documento de identidad.
a.2) Que no cuenten con afiliación política y no se encuentren afectos a las incompatibilidades señaladas en el *artículo 16: Impedimentos para los funcionarios* de la Ley N° 26487, Ley de Orgánica de la Oficina Nacional de Procesos Electorales.
a.3) Otras que se determinen de acuerdo a las funciones que va a realizar.

b) La GCPH debe establecer en los acuerdos contractuales de empleo las cláusulas de confidencialidad, declaración de responsabilidades respecto a la seguridad de la información, cláusulas respecto a las leyes de derecho de autor o protección de datos, según corresponda. Dichos acuerdos contractuales deben estar vigentes por lo menos tres (3) años después de finalizado el contrato.

6.2.2. Durante el empleo

La GCPH o la GIEE para el caso de personal de la ODPE, deben:

a) Incluir en su plan de inducción y capacitación aspectos de seguridad de la información según las políticas, normas y procedimientos relevantes relacionados, en coordinación con la GGC.

b) Asegurar, en coordinación con la GGC, que las inducciones y capacitaciones de seguridad de la información sean recibidas por el personal.

La GCPH debe:

c) A través de la Secretaria Técnica de Procedimientos Administrativos Disciplinarios[1] se procederá, previa presentación de una denuncia o informe ante los órganos competentes, con la aplicación del Procedimiento Administrativo Disciplinario, que establece la Ley del Servicio Civil y su reglamento, ante incumplimientos o faltas tipificadas en estos.

d) Realizar, en coordinación con la GGC, la inducción y de manera permanente la actualización de conocimientos relacionados con la seguridad de la información en el desarrollo de las funciones del personal de la ONPE.

El personal debe:

e) Cumplir con la política, objetivos y lineamientos de seguridad de la información emitidas en la presente directiva, así como con otras relacionadas. En caso de evidenciar una acción o evento que atente contra estas normas, debe comunicárselo al OSI.

6.2.3. Cese del empleo o cambio de puesto de trabajo

a) El personal, cuando cambie de puesto o termine su relación contractual con la institución, debe entregar o poner a disposición de su jefe inmediato (o a quien éste designe formalmente) todos los documentos físicos y electrónicos encargados y demás activos asociados a la información que se les haya entregado para el cumplimiento de sus funciones, así como su fotocheck e indumentarias que identifiquen a la institución. Corresponde al jefe inmediato verificar la información entregada por el personal.

b) La GCPH debe solicitar a la GITE, a la brevedad posible, la cancelación de las cuentas de acceso a los sistemas informáticos del personal cuya relación contractual se haya extinguido.

c) La GCPH deberá informar a la OSDN a la brevedad posible, la baja del personal que termine su relación contractual con la institución; y la actualización de la base de datos del personal para el control de acceso físico a las diferentes sedes de la institución.

d) La GITE y la OSDN deben, en lo que les corresponda, remover o bloquear todos los accesos físicos (permisos de acceso a lugares o sitios físicos, por

[1] Cargo designado por el titular de la institución. Las referencias de este cargo se encuentran en la Directiva Nº 02-2015-SERVIR/GPGSC Régimen Disciplinario y Procedimiento Sancionador de la Ley N° 30057, Ley del Servicio Civil.

ejemplo: llaves de puertas o de armarios) y lógicos (permisos de acceso a sistemas o información almacenada electrónicamente, por ejemplo: usuarios y claves de red, o de un sistema de información) cuando el personal cambie de puesto o termine su relación contractual con la institución.

6.3. Gestión de Activos

6.3.1. Responsabilidad de los activos

Los responsables de los órganos de la institución deben asegurar que se elabore un inventario de activos de información.

Los propietarios de activos deben:

a) Mantener actualizado un inventario de sus activos de información, así como de clasificarlos (ver 6.3.2 Clasificación de la Información).

b) Informar el inventario de activos de información dentro del plazo de 48 horas, después de efectuada la actualización del mismo, al CGSI y a la SG

c) Asegurar el adecuado tratamiento y protección de los activos de información a su cargo.

Los usuarios deben:

d) Usar de forma ética y eficiente los activos de información que le sean asignados solo y exclusivamente para fines laborales, en cumplimiento con el marco normativo para evitar daños operativos, a la imagen o a otros intereses de la institución.

e) Evitar el uso de equipos informáticos de pertenencia personal para desempeñar sus actividades laborales.

f) Evitar la exposición o divulgación de la información confidencial, reservada o secreta que manejen, guardándolo bajo llave o caja fuerte, según amerite.

6.3.2. Clasificación de la información

a) En concordancia con la Ley de Transparencia y Acceso a la Información Pública, es responsabilidad del titular de la ONPE o de los funcionarios designados por este, clasificar su información en: información secreta, reservada. Según Resolución Jefatural 086-2016-J/ONPE, se delegó a Secretaría General la facultad de clasificar y desclasificar como información SECRETA y RESERVADA los activos de información en posesión de la ONPE.
Los propietarios de activos son responsables de clasificar la información que manejan en cada proceso o proyecto, de acuerdo a lo establecido en la Ley de Transparencia y Acceso a la Información Pública.

Los propietarios de los activos deberán etiquetar la información según la clasificación realizada, y que sea conforme a los lineamientos que establezca la institución.

b) Los propietarios de activos deben asegurar el manejo de sus activos de acuerdo a lo siguiente:

Para la información clasificada como secreta y reservada
i. Se debe ubicar en un ambiente que cuente con acceso biométrico o de acceso restringido con resguardo de un personal asignado por el órgano que custodia dicha información.
ii. Su almacenamiento debe ser mínimamente dentro de una caja fuerte (o algún otro mecanismo de seguridad similar) o ser cifrado (preferentemente con la última versión tecnológica existente), según corresponda.
iii. No se debe obtener copias físicas o electrónicas bajo ninguna circunstancia.
iv. Por lo tanto, tampoco se debe enviar por ningún medio electrónico.
Para la información clasificada como confidencial
v. Se debe ubicar en un ambiente que cuente con acceso restringido, registrándose los accesos a estos ambientes.
vi. Su almacenamiento debe ser mínimamente bajo llave (o algún otro mecanismo de seguridad similar) o ser cifrado (con la última versión tecnológica compatible con los sistemas institucionales), según corresponda.
vii. Se debe controlar las copias físicas o electrónicas registrándose, como mínimo, el número de identificación de la copia y de la persona quien la recibe.
viii. **Su envío solamente debe ser por correo electrónico institucional** y encriptado a direcciones de correos electrónicos institucionales autorizados por el propietario del activo.

6.3.3. Gestión de medios de almacenamiento removibles

Los responsables de los órganos de la institución deben autorizar a su personal el uso de medios de almacenamiento removibles, en caso lo amerite. El cumplimiento de esta autorización está a cargo de la GITE.

6.4. Control de Accesos

Los propietarios de activos de información, incluyendo a la información en sí, deben asegurar que estos reciban los controles de accesos necesarios y adecuados sin degradación del flujo de las actividades de los procesos.

6.4.1. Gestión de acceso de usuario

Los responsables de los órganos de la institución deben:

a) Autorizar, y luego solicitar a la GITE el acceso a los sistemas de información para su personal, proveedor de servicios y terceros, indicando los niveles de acceso o privilegios.

b) Deberán solicitar a la GITE la cancelación de las cuentas de acceso a los servicios de tecnologías de la información otorgadas a proveedores y terceros una vez concluida la relación contractual o necesidad del servicio.

La GCPH debe:

a) Solicitar a la GITE la baja de las cuentas de acceso del personal cuando finalice la relación contractual.

La GITE debe:

b) Confirmar con la GCPH la relación contractual antes de otorgar el acceso a los sistemas de información solicitados.

c) Cancelar las cuentas de acceso una vez finalizada las labores del personal cesado, teniendo dos días hábiles de plazo a partir de la comunicación de la GCPH. Asimismo, cancelar las cuentas de acceso de proveedores y terceros previa solicitud del órgano que solicitó el servicio.

d) Coordinar la baja de las cuentas de acceso de los administradores de sistemas de información antes de su cese.

e) Llevar un registro del personal que cumple el rol de administrador de sistema de información.

Los administradores de sistemas de información deben:

f) Guardar el registro de la solicitud de autorización de acceso.

g) Revisar y mantener actualizado permanentemente los registros de cuentas de acceso a los sistemas de información que administran en coordinación con los Responsables del Sistema de Gestión de cada órgano.

El OSI debe:

h) Revisar semestralmente, en coordinación con el Responsable de la Seguridad Tecnológica, las cuentas de acceso de los administradores de los sistemas de información.

i) Revisar semestralmente, en coordinación con los Responsables del Sistema de Gestión de cada órgano, las cuentas de acceso de los usuarios de los sistemas de información.

6.4.2. Responsabilidades del usuario

Los usuarios de los sistemas de información[2] son responsables del uso correcto de las cuentas asignadas para el acceso a los sistemas o servicios informáticos de la institución, por lo tanto deben:

a) Cambiar las contraseñas proporcionadas por los administradores de los sistemas de información antes de su primer inicio de sesión.

b) Mantener la confidencialidad de su contraseña (no compartirlas) y cambiar la misma si tiene algún indicio de su vulnerabilidad.

c) Seleccionar una contraseña que cuente con un nivel adecuado de complejidad, siguiendo las siguientes consideraciones:

c.1) Debe tener una longitud mínima de ocho caracteres.
c.2) Debe ser una combinación de letras mayúsculas, minúsculas y números. De preferencia, incluir también caracteres especiales, evitando así el uso de palabras comunes o datos personales.

d) Evitar anotar sus contraseñas en medios físicos o electrónicos, a menos que éste cuente con algún control criptográfico.

e) Acceder a los sistemas de información de la ONPE solo desde equipos asignados por la institución.

6.4.3. Control de acceso a los sistemas de información

a) Los administradores de sistemas de información deben configurar tales sistemas considerando lo siguiente:

a.1) Que obliguen a los usuarios a cambiar su contraseña cuando ingrese por primera vez.
a.2) Que bloqueen el acceso por 15 minutos luego de 5 intentos fallidos.
a.3) Que permitan a los usuarios cambiar su contraseña cuando lo requiera.
a.4) Que obliguen a los usuarios cambiar su contraseña como máximo cada 60 días. En el caso de cuentas con privilegios de administrador, estas deben cambiarse cada 6 meses.
a.5) Que guarden un registro de los intentos fallidos y exitosos de acceso.
a.6) Para los sistemas de información de acceso desde fuera de las instalaciones, adicionalmente que bloqueen las cuentas que superen los 5 intentos fallidos de acceso.

b) Los administradores de sistemas de información deben solamente asignar a cada usuario una cuenta de acceso por sistema de información, salvo por razones de operación estrictamente justificados.

[2] Para las Soluciones Tecnológicas de Voto Electrónico corresponde a la GITE implementar los controles de seguridad necesarios y adecuados con la finalidad de asegurar la confidencialidad, integridad y disponibilidad de la información.

c) La GITE debe asegurar que sus desarrolladores solo tengan acceso a aquellas partes del código fuente del software que sea necesario para su trabajo.

6.5. Criptografía

El personal debe:

a) Enviar de manera encriptada la información electrónica que no sea de carácter público almacenada en medios tecnológicos, previa autorización de su propietario. Solicitar el apoyo de la GITE de ser necesario.

La GITE debe:

b) Implementar en los sistemas de información de acceso desde fuera de las instalaciones de la institución controles criptográficos que permitan:

b.1) Validar la integridad o identidad de los sistemas de información.
b.2) Una conexión segura para el caso que los sistemas de información requieran autenticación de los usuarios.
b.3) Proteger la integridad y confidencialidad de la información (este último de ser el caso) desde su transmisión hasta su recepción.

c) Encriptar la información que no sea de carácter público almacenada en las bases de datos.

d) Asegurar que los controles criptográficos de los sistemas de información adquiridos o desarrollados cumplan con los estándares nacionales o internacionales.

e) Asegurar que el medio de almacenamiento de los certificados digitales emitidos por una EC cumple con los estándares establecidos por la AAC.

6.6. Seguridad física y ambiental de las instalaciones

La ONPE tomará las medidas físicas y ambientales que sean necesarias y adecuadas dentro y fuera de sus instalaciones para proteger su información, junto con sus activos de tratamiento asociados más relevantes, contra riesgos que atenten contra su confidencialidad, integridad y disponibilidad.

6.6.1. Seguridad asociada a las instalaciones

La OSDN debe a nivel nacional:

a) Realizar la evaluación correspondiente a fin de mantener asegurado el perímetro de las instalaciones, sobre todo, de las de tratamiento de información que no sea de carácter público. Asimismo, previa información de los órganos, debe evaluar y determinar los controles de seguridad a implementar por los órganos para la custodia de los activos de tratamiento de información.

b) A través de los Agentes de Vigilancia Privada – AVP, se verificará que el personal, proveedores y terceros, tanto en el ingreso como en su permanencia, porten visiblemente su fotocheck (laboral o visitante). Asimismo, debe coordinar con los demás órganos al respecto para que sea apoyada en los lugares en donde no se cuente con personal de seguridad y vigilancia.

c) A través de los Agente de Vigilancia Privada – AVP, se examinará el material que ingresa a la zona de despacho y recepción de materiales para detectar posible material explosivo, químico o algún otro peligroso antes que sea trasladado al ambiente de destino. Asimismo, coordinar con los demás órganos al respecto para que sea apoyada en los lugares en donde no se cuente con personal de seguridad y vigilancia.

Los responsables de los órganos de la institución deben:

d) Asegurar que sean registrados todos los accesos a las instalaciones no ocupadas permanentemente en donde se trate información que no sea de carácter público.

e) Asegurar que solamente exista una llave de contingencia de la puerta de acceso a las instalaciones de tratamiento de información que estén bajo su responsabilidad, y que sea custodiada por la OSDN.

f) Asegurar que los equipos de registro fotográfico, video, audio u otros, tales como cámaras en dispositivos móviles, no sean usados en los ambientes que determine, a menos que otorgue su autorización.

g) Asegurar que los proveedores y terceros que accedan a las instalaciones de tratamiento de información sensible solo usen el material estrictamente necesario para llevar a cabo las actividades acordadas.

h) Asegurar que los proveedores o los terceros no ingresen a las instalaciones de tratamiento de información sensibles sin la presencia del personal a cargo o de su representante.

i) Asegurar que los materiales peligrosos y combustibles sean almacenados en un área diferente a las instalaciones de tratamiento de información.

j) Asegurar que las puertas y ventanas exteriores e interiores estén protegidas contra accesos no autorizados, sobre todo en horas no laborales.

6.6.2. Seguridad asociada a los equipos institucionales

La OSDN debe:

a) Inspeccionar que los centros de datos cuenten con señaléticas de seguridad.

La GITE debe:

b) Monitorizar la temperatura y humedad de los centros de datos.

c) Asegurar el funcionamiento de los equipos de respaldo de energía eléctrica cuando falle o se corte el suministro de energía eléctrica principal.

d) Asegurar que durante el mantenimiento que realicen a los equipos servidores, no haya posibilidad de fuga de información.

e) Asegurar que se efectúe el mantenimiento a los equipos servidores, equipos de respaldo de energía eléctrica, de control de temperatura, entre otros, ubicados en los centros de datos.

f) Asegurar el mantenimiento de los equipos informáticos del personal.

g) Asegurar que los equipos informáticos institucionales involucrados en la prestación y realización de transacciones de gobierno electrónico, de acuerdo a la Ley de Certificados y Firmas Digitales, cuenten con algún tipo de certificado de dispositivo seguro emitidos por una EC debidamente acreditada ante el INDECOPI.

h) Asegurar que los medios de almacenamiento institucionales que custodian y que van a ser reutilizados, reemplazados o desechados —y, a su vez, que contengan información que no sea de carácter público o que contengan software con copia registrada (copyright)— sean destruidos físicamente o que su contenido sea borrado de manera irreversible.

Los responsables de los órganos de la institución a cargo del Archivo Central, del Archivo Electoral, y de otros espacios en donde se custodie información física o electrónica deben:

i) Asegurar que se efectúe el mantenimiento a los equipos e instrumentos que permiten la conservación de los medios en donde se soporta la información física y electrónica custodiada.

Los usuarios deben:

j) Efectuar, o solicitar a la GITE que puedan efectuar, una copia de respaldo de su información antes que el equipo informático institucional que le fue asignado sea reutilizado, reemplazado, desechado o pase a mantenimiento, y luego custodiarla de acuerdo a su nivel de clasificación. En caso de información que no sea de carácter público, esta debe ser eliminada de su equipo informático.

k) Evitar la apertura de los equipos informáticos; es decir, evitar acceder a los componentes internos de estos (solo el personal de soporte técnico podría hacerla en caso corresponda).

l) Evitar transportar equipos informáticos institucionales dentro o fuera de las instalaciones.

m) Asegurar que los medios de almacenamiento que custodian y que van a ser reutilizados, reemplazados o desechados —y, a su vez, que contengan

información que no sea de carácter público o que contengan softwares con copia registrada (copyright)— sean destruidos físicamente o que su contenido sea borrado de manera irreversible.

6.7. Seguridad de las operaciones

La ONPE tomará las medidas necesarias y adecuadas para asegurar la operación correcta y segura de sus activos de información y para prever la pérdida permanente de su información de negocio y de soporte.

La GGC debe:

a) Proponer a la GG los controles de seguridad de la información cuando se originen cambios en la organización y procesos de negocio.

La GITE debe:

b) Restringir el acceso de videos y música en línea (on-line) que no son de propósito laboral.

c) Asegurar que durante el ciclo de desarrollo de software se trabaje en ambientes de desarrollo, prueba y producción por separado y que se definan las reglas de transferencia a cada tipo de ambiente.

d) Asegurar que los equipos informáticos cuenten con un software contra códigos maliciosos y de actualización periódica.

e) Orientar a los usuarios sobre cómo afrontar un evento u ocurrencia de infección de virus informático.

f) Obtener periódicamente y etiquetar las copias de respaldo de información almacenada en los equipos servidores, así como efectuar las pruebas de restauración de la información de acuerdo a su plan respectivo (si se trata de información que no sea de carácter público, se debe contar con la presencia del Propietario o del representante que este designe).

g) Encriptar las copias de respaldo de la información que no sea de carácter público que obtenga desde los equipos servidores.

h) Ubicar las copias de respaldo de información en otro(s) local(es) distante(s) de la institución que cuenten con armarios seguros —sin perjuicio de contar también con sus duplicados en los mismos locales—, el(los) cual(es) debe(n) contar con controles de seguridad física y con adecuadas condiciones de temperatura y humedad.

i) Efectuar, a solicitud del personal, las copias de respaldo de la información almacenada en sus equipos informáticos.

j) Implementar los controles que aseguren que los eventos de sistemas de información (log) no sean manipulados por quienes los administran, tal como

la activación de registros de auditoría. Obtener las copias de seguridad de estos eventos (log) mensualmente.

k) Implementar controles de protección de privacidad de los datos personales almacenada en los eventos de sistemas de información (log).

l) Programar un análisis de vulnerabilidades técnicas de los sistemas de información más relevantes para cada proceso electoral que organice la institución; y programar las acciones necesarias para prevenir o mitigar los riesgos que se identifiquen producto de éste análisis.

m) Restringir el otorgamiento de privilegios sobre el manejo de los equipos informáticos al personal cuya función no la requiere para evitar instalaciones de software que pueden acarrear incidentes de seguridad de la información y violaciones de derechos de propiedad intelectual.

n) Restringir que las pruebas a los sistemas de información durante una revisión estén limitadas a accesos de solo lectura al software. Asimismo, asegurar, en caso se requiera acceso de escritura, se efectúe una copia de respaldo, y luego se elimine o se resguarde, según sea el caso, al culminar la revisión.

o) Asegurar que las revisiones a los sistemas de información a efectuar con datos confidenciales sean dentro de las instalaciones de la institución acompañado por el responsable del sistema de información revisado; no está permitido la entrega de este tipo de datos.

p) Asegurar que la capacidad y desempeño de la infraestructura de TI, pueden soportar eficientemente las demandas de los servicios de TI y recursos tecnológicos requeridos por la ONPE.

Los usuarios deben:

q) Realizar la copia de respaldo de su información con apoyo del personal de soporte técnico, y deben guardarlo bajo las condiciones de acuerdo a su nivel de clasificación (referencia: 6.3.2. Clasificación de la información).

r) Solicitar a la GITE el almacenamiento de su información necesaria o indispensable en el servidor de archivos.

s) Acatar las directrices de buen uso de software institucional emitidas por la GITE.

6.8. Seguridad relacionada a las comunicaciones

La ONPE implementará las medidas necesarias y adecuadas en los medios de transporte y de reproducción, tecnológicos o no, de la información, de tal manera que solo sea emitida y recibida íntegramente por las personas apropiadas en el momento y lugar oportunos.

La GITE debe:

a) Asegurar que los identificadores otorgados a las redes inalámbricas de la institución no contengan relación con esta. Asimismo, que el acceso a estas redes sea configurado con contraseña encriptada.

El personal debe:

b) Asegurar que la información que no sea de carácter público que vayan a adjuntar a su correo electrónico institucional solamente sea enviada con controles criptográficos según su nivel de clasificación (referencia: 6.3.2 Clasificación de la información). Bajo ningún motivo deben usar medios de mensajería que no sean institucionales.

c) Acatar las directrices de buen uso de correo electrónico institucional emitidas por la GITE.

d) Asegurar que la información que no sea de carácter público solamente sea compartida entre los usuarios autorizados por el propietario de la información.

e) Evitar que la información que no sea de carácter público sea abandonada en las instalaciones de impresión (impresoras, fotocopiadoras, faxes) o que sea grabada en máquinas contestadoras.

f) Evitar conversaciones de temas confidenciales en lugares públicos u oficinas abiertas.

g) Lacrar los sobres que envíen si contienen información que no sea de carácter público.

Los responsables de los órganos de la institución deben:

h) Asegurar el uso de un acuerdo de confidencialidad y no divulgación cuando requieran transferir información que no sea de carácter público con algún otro órgano, unidad orgánica o entidad.

6.9. Adquisición, desarrollo y mantenimiento de sistemas de información

6.9.1. Requerimientos de seguridad de los sistemas de información

Los líderes usuarios de los sistemas de información deben:

a) Identificar y documentar con asesoría de la GITE, los requerimientos de seguridad en las etapas iniciales del proyecto de adquisición o desarrollo de software.

La GITE debe:

b) Asegurar que los cambios a realizar, solicitados previa y formalmente por los líderes usuarios, no causen riesgos de seguridad (de ocurrir, debe deshabilitarlos para su posterior subsanación).

c) Validar nuevamente, en caso se hayan producido cambios en el software, los datos de entrada y los datos de salida esperados.

6.9.2. Seguridad en el desarrollo y en los procesos de soporte

La GITE debe:

a) Involucrar la seguridad en las metodologías de desarrollo de software que se usen, así como implementar el control de versiones.

b) Asegurar que las actualizaciones de los componentes del sistema operativo no interrumpan la funcionalidad de los sistemas de información adquiridos o desarrollados.

6.9.3. Datos de prueba

La GITE debe:

a) Asegurar que los datos personales utilizados en los ambientes de desarrollo y de prueba sean sometidos a procedimientos de anonimización o disociación antes de su uso.

b) No hacer uso de datos personales sensibles para propósitos de pruebas.

6.10. Relación con proveedores

6.10.1. Seguridad con relación a los proveedores

Los responsables de los órganos de la institución que requieren la contratación de bienes y servicios relacionados con el acceso, procesamiento, almacenamiento, comunicación y otro tipo de tratamiento de información deben:

a) Asegurar la incorporación de requerimientos de seguridad (organizativos, jurídicos y técnicos) en los términos de referencia con asesoría de la GITE o del OSI. Tales requerimientos principalmente deben estar asociados a la transferencia de o acceso a información, la resolución de incidentes, las medidas de contingencia o a los controles de cambios, así como el derecho para efectuar auditorías al servicio brindado.

b) Asegurar que el proveedor (directo y subcontratado) que tratará información que no sea de carácter público conozca las políticas y procedimientos de seguridad que le sean aplicables, y que firme un acuerdo de confidencialidad y de no divulgación.

c) Asegurar que no manipulen cualquier tipo de documento no relacionado al motivo del servicio contratado, así como su copia (transcripción, fotocopia, fotografía, entre otros).

La SG, de acuerdo a lo establecido en los artículos 15, 16 y 17 de la Ley de Transparencia y Acceso a la Información Pública, para la información que no sea de carácter público que ingrese a la institución, debe:

d) Registrar solamente los datos que figuran en el sobre y no escanear o fotocopiar la información contenida en él.

e) Entregar la información entrante manteniendo el sobre cerrado al órgano destinatario, registrando previamente la hora de salida de la información de la mesa de partes.

6.10.2. Gestión de entrega de servicio del proveedor

a) Los responsables de los órganos de la institución deben asegurar el seguimiento a los niveles de desempeño del servicio, así como el cumplimiento de los requerimientos de seguridad de la información incorporados en los términos de referencia.

6.11. Gestión de incidentes de seguridad de la información

a) El personal, proveedores de servicios y terceros deben reportar todo tipo de eventos relacionados a la seguridad de la información, tecnológicos o no, al punto de contacto indicado en los procedimientos relacionados.

b) Los usuarios deben reportar a la OSI indicios de debilidades de seguridad de los sistemas de información. No deben intentar comprobar estos indicios para prevenir daños a la institución.

c) La OSI en coordinación con los órganos involucrados, deben evaluar mensualmente los eventos reportados para determinar si se clasifican como incidentes de seguridad de la información, analizando su causa raíz, probabilidad e impacto.

d) La GITE debe reportar los incidentes informáticos a la PeCERT según lo señalado en el procedimiento de esta autoridad, así como asegurar que se atiendan los avisos de alerta que envía esta.

6.12. Seguridad la información asociada a la continuidad de negocio

La ONPE asegurará que la confidencialidad, integridad y disponibilidad de su información no se degraden durante un hecho catastrófico de origen natural o humano.

6.12.1. Continuidad de la seguridad de la información

a) El Grupo de Trabajo de la Gestión del Riesgo de Desastres de la ONPE a través del "Plan de Continuidad Operativa", en coordinación con los demás órganos de la ONPE, deben elaborar un plan que busque proteger físicamente los activos de información, principalmente a los que acarreen catastróficos perjuicios; y deben asegurar la continuidad de los sistemas de información ante desastres naturales y ocasionados por el hombre, incluyendo aspectos relacionados a la continuidad de la confidencialidad, integridad y disponibilidad de la información, de tal forma que se mantengan sus requerimientos también en situaciones adversas.

b) El Grupo de Trabajo de la Gestión del Riesgo de Desastres de la ONPE a través del "Plan de Continuidad Operativa", en coordinación con los demás órganos, deben implementar lo contemplado en el plan relacionado a la continuidad de las operaciones de la institución, cuyo contenido debe incorporar, además de los requisitos legales aplicables, la estructura organizativa, procedimientos de respuesta y restauración, así como los controles que aseguren el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.

c) La GITE, en coordinación con órganos propietarios de los sistemas de información, debe efectuar pruebas del plan de continuidad para verificar la eficacia de los controles por lo menos una vez al año o una vez en cada proceso electoral que organice la institución.

6.12.2. Redundancias

a) La GITE debe aplicar la redundancia a nivel de enlace de telecomunicaciones, servidores, base de datos, y otros recursos tecnológicos que asegure la continuidad de los sistemas de información que considere indispensables o necesarios. Asimismo, debe comprobar que los componentes redundantes operan ante la caída de los principales.

b) Los dueños de los procesos, en coordinación con la GGC y la GITE, deben establecer los requisitos de seguridad de la información y de continuidad para sus procesos considerando las situaciones adversas a las que pueden estar expuestas.

6.13. Cumplimiento

6.13.1. Cumplimiento de los requisitos legales y contractuales

La GITE debe:

a) Impedir que se instale software que atente contra los derechos de propiedad intelectual.

b) Llevar un registro de licencias de software y mantener las evidencias de estas.

c) Implementar controles que aseguren que el número máximo de usuarios permitidos con licencias no sea excedido.

Todos los órganos y unidades orgánicas que difundan o compartan documentos ofimáticos deben:

d) Eliminar la información de privacidad almacenada ocultamente en el software ofimático.

La SG debe:

e) Realizar los trámites de inscripción de los bancos de datos personales creados, así como para los que se generen.

Todos los órganos y unidades orgánicas que tratan datos personales de los electores o potenciales electores deben efectuar su tratamiento de acuerdo a las normas legales vigentes y lo estipulado en la Política de Protección de Datos Personales. En esta línea deben:

f) Obtener el consentimiento libre, previo, expreso, informado e inequívoco del titular para el tratamiento de sus datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar o transmitir dichos datos personales en el marco de las actividades de la institución.

g) Gestionar la implementación de los controles de tratamiento y de protección de los datos personales que administran según las directivas emitidas por la APDP y los documentos normativos de la institución.

h) Acatar las disposiciones del Encargado de Banco de Datos Personales para el cumplimiento de la LPDP.

La GITE debe:

i) Implementar los controles de protección de los datos personales almacenada en las bases de datos o que se transmiten electrónicamente según lo establecido en la directiva emitida por la APDP.

Todos los órganos y unidades orgánicas que reciban o importen datos personales deben:

j) Implementar las medidas de seguridad definidas por el emisor o exportador de datos personales. La aceptación de la implementación de las medidas de seguridad debe establecerse por escrito mediante cláusulas contractuales u otro instrumento jurídico.

Todos los órganos y unidades orgánicas que emitan o exporten datos personales deben:

k) Disponer cláusulas contractuales u otro instrumento jurídico en los que se establezcan cuando menos las mismas obligaciones a la que se deben encontrar sujetos los receptores o importadores de los datos personales.

La GCPH debe:

l) Cumplir con las disposiciones de seguridad de los bancos de datos personales de la administración del personal emitidas por la directiva de la APDP.

6.13.2. Revisión independiente de la seguridad de la información

La GGC debe:

a) Planificar las auditorías internas y externas de seguridad de la información para que se lleven a cabo una vez al año mínimamente y con auditores independientes al proceso a auditar.

b) Reportar los resultados de la revisión independiente a los interesados para la atención de los hallazgos encontrados.

7. MECÁNICA OPERATIVA

Los procedimientos e instructivos que se elaboren deben cumplir lo dispuesto en la presente directiva.

8. CUADRO DE CONTROL DE CAMBIOS

Versión Anterior	Fecha de Aprobación	Sección / Ítem	Categoría N: Nuevo M: Modificado E: Eliminado	Principales cambios realizados con respecto a la versión anterior
00	22/12/2015	Título	M	Se cambia la Directiva DI03-GGC/GC Política de Seguridad de la Información (versión 00) aprobada por Resolución Jefatural N° 000370-2015-J/ONPE del 22/12/2015 por la DI04-GGC/GC Lineamientos de Seguridad de la Información (versión 00)
00	22/12/2015	Título	E	Extrayendo del documento el numeral 6.1. Política general de seguridad de la información de la DI03-GGC/GC.