CONTENIDO

I. TÉRMINOS DE REFERENCIA

1. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de Mensajería Express Lima Metropolitana y Callao.

2. FINALIDAD PÚBLICA

El servicio de Mensajería Express Lima Metropolitana y Callao servirá como apoyoa las dependencias de la ONP para la notificación de las comunicaciones a los administrados, entidades, personas naturales o jurídicas.

3. VINCULACIÓN CON EL POI

Este servicio está vinculado dentro de la actividad del Plan Operativo Institucional AOI00005500331 Evaluación de la notificación oportuna de resoluciones y/o reconocimientos de prestaciones previsionales.

4. OBJETIVOS DE LA CONTRATACIÓN

Contratar el Servicio de Mensajería Lima Metropolitana y Callao, que deberá cubrir la recepción de los documentos emitidos por el Sistema Nacional de Pensiones a cargo de la ONP, así como documentación administrativa para su distribución y entrega a los administrados, entidades, personas naturales o jurídicas.

5. BASE LEGAL

- Decreto Supremo 082-2019-EF, que aprueba el Texto Único Ordenado de la Ley 30225, Ley de Contrataciones del Estado.
- Decreto Supremo 344-2018-EF, que aprueba el Reglamento de la Ley 30225, Ley de Contrataciones del Estado.
- Ley 31365, Ley de Presupuesto del Sector Público para el Año Fiscal 2022.
- Ley 31366, Ley de Equilibrio Financiero del Presupuesto del Sector Público para el año fiscal 2022.
- Ley 31367, Ley de Endeudamiento del Sector Público para el año fiscal 2022.
- Decreto Supremo 004-2019-JUS, que aprueba el Texto único Ordenado de la Ley 27444, Ley del Procedimiento Administrativo General.
- Decreto Supremo 21-2019-JUS, que aprueba el Texto Único Ordenado de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.
- Decreto Supremo 072-2003-PCM, que aprueba el Reglamento de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.
- Código Civil.
- Directivas y Opiniones del OSCE.
- Plan para la Vigilancia, prevención y control del COVID-19 en el trabajo de la ONP.

Las referidas normas incluyen sus respectivas modificaciones, de ser el caso.

6. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

La descripción y las características de los servicios de mensajería son los siguientes:

Mensajería Express Lima Metropolitana y Callao

6.1 Actividades

6.1.1. Fases del Servicio

6.1.1.1. Fase Pre Operativa

Esta fase tiene como función asegurar el correcto inicio de operaciones en lo concerniente al Servicio de Mensajería.
El inicio de la fase Pre Operativa será a partir del día siguiente de la suscripción del contrato por un plazo máximo de 10 días calendario.

La Fase Pre Operativa comprende las siguientes acciones:

Cuadro Nº 01

N°	ACCIONES	RESPONSABLE
1	Designar al representante encargado de coordinar y realizar las acciones establecidas para la presente fase con plena satisfacción de las partes.	Supervisión ONP – Contratista
2	Presentar al supervisor(a) quien será el personal clave establecidos en los "Requisitos de Calificación", que brindará soporte necesario para la ejecución del servicio durante toda la Fase Operativa.	Contratista
3	Presentar la relación del personal que realizará el recojo de la documentación en la ONP a nivel Local, contemplando como mínimo: - Nº DNI - Apellidos y Nombres - Fecha de Nacimiento - Edad	Contratista
4	Designar a los representantes que participarán en el Comité Operativo en la Fase Operativa.	Supervisión ONP – Contratista
5	La Supervisión entregará al contratista los formatos de la entrega de la correspondencia y devolución de los cargos	Supervisión ONP
6	Proveer de los suministros[1] necesarios para la ejecución del servicio.	Contratista
7	Brindar acceso de consulta y capacitación de uso a los usuarios que defina la ONP, en el aplicativo o Web que permite verificar el estado de la Mensajería.	Contratista

[1] Suministros – Formatos de Aviso de Visita y Acta de Notificación – Ver Anexo Nº 04.

8	Entregar una guía o manual a ONP, sobre el uso del aplicativo o web	Contratista
9	Entrega de la "Declaración Jurada- Cumplimiento de políticas de seguridad de la información" y "Compromiso de Confidencialidad"	Contratista
10	Realizar la suscripción de un Acta Preoperativa que contemplara las Acciones realizadas en la presente Fase con plena satisfacción de las partes (finalización de la fase Pre Operativa).	Supervisión ONP – Contratista

6.1.1.2. Fase Operativa

El inicio de la fase operativa deberá darse a partir del día siguiente de la culminación de la Fase Pre Operativa.

La duración de la Fase Operativa es de hasta 1,096 días calendario o agotar el monto contractual, lo que suceda primero.

6.2. Proyectos en Desarrollo

La ONP como parte de la mejora continua de sus procesos desarrolla y genera nuevos proyectos, los mismos que pueden influir en la operatividad de la gestión del presente servicio. En tal sentido en caso la institución realice cambios en la operatividad de servicio, informará con la debida anticipación a los Contratistas, de presentarse situaciones que afecten al alcance del presente servicio, se aplicará la normativa de contrataciones del estado y su reglamento (prestaciones adicionales, reducción de prestaciones, ampliación de plazo, modificación del contrato, entre otras que resulten aplicables).

6.3. De los procedimientos

El procedimiento para la notificación presencial de resoluciones, notificaciones u otros (actos administrativos), será el establecido en la Ley Nº 27444, Ley del Procedimiento Administrativo General, Artículo 21 Régimen de la Notificación personal.

6.4. Del control de calidad

La ONP podrá realizar auditorías, inspecciones y/o evaluaciones inopinadas al proceso operativo; sin previo aviso, según la periodicidad que la ONP lo estime conveniente, por su cuenta o a través de terceros para verificar el cumplimiento del servicio a cargo de El Contratista. Estas acciones podrán incluir la evaluación de criterios de eficiencia, calidad, productividad y oportunidad, en un proceso de mejora continua.

Asimismo, la ONP podrá realizar revisiones sin previo aviso, a los documentos (cargos, actas de notificación entre otros), a fin de evaluar la calidad y el cumplimiento del servicio prestado por El Contratista.

El procedimiento a seguir será el siguiente:

- En cualquier día, considerado de manera aleatoria y sin necesidad de

coordinaciones previas con el contratista, la ONP por intermedio del personal supervisor que evalúa el servicio revisará los documentos recibidos por el Contratista, a fin de efectuar la verificación de los datos (Nombres/Apellidos/DNI/Parentezco/Firma/Fecha de recepción), contemplados en el documento, cuya información ha sido proporcionado por el contratista.

- Una vez efectuado el primer punto, y de ser conforme se procederá a la llamada telefónica, registrada por la/el administrada/o en los sistemas de la ONP. Donde se confirmará la recepción de la correspondencia entregada al administrado por parte del contratista.
- El resultado de la auditoría, de la inspección y/o la evaluación al desempeño del proceso operativo será remitido a El Contratista, a fin de que implemente las acciones de prevención y mejora.
- En caso de encontrar inconsistencias, errores, irregularidades y/o incumplimientos del contrato que se haya suscrito, es facultad de la ONP la aplicación de las penalidades que correspondan, de acuerdo a los plazos señalados en los presentes términos de referencia.

6.5. De las comunicaciones

Los Contratistas deben considerar que de ser necesario la ONP requerirá desarrollar reuniones de control y/o coordinación, en sede central de ONP:

- Comité Operativo: En estas Reuniones se tratarán todos los temas referentes a asuntos de relevancia respecto a la operación del servicio y se realizarán a requerimiento de la ONP, como consecuencia de dicha reunión se elaborará un Acta de Comité.

Los participantes (como mínimo un (1) integrante de la Supervisión del servicio de la ONP y un (1) supervisor del contratista) de estos Comités se definirán en la Fase Pre Operativa y se podrán actualizar en la Fase Operativa.

Asimismo, en la Fase Preoperativa los Contratistas deberán proporcionar la información actualizada de correos electrónicos, teléfonos, anexos y números de equipos móviles del personal responsable de los procesos, y de presentarse alguna modificación, esta deberá ser comunicada a la ONP con un día hábil de anticipación.

- Comunicación formal: Es la comunicación efectuada mediante carta, oficio, informe o correo electrónico.

6.6. Servicio de Mensajería Lima Metropolitana y Callao

Tiene como objetivo gestionar de manera eficiente el envío de la correspondencia de la ONP de Lima Metropolitana y la Provincia Constitucional del Callao (según se detalla en el Anexo Nº 01) con el retorno de un cargo de entrega.

Este servicio llevará a cabo las labores relacionadas al envío de la correspondencia al cliente y/o al usuario a nivel local.

Cuadro Nº 03

N°	DESCRIPCIÓN DE SERVICIO	PROPIETARIO DE LA DOCUMENTACIÓN	RESPONSABLE DEL SERVICIO	RESULTADO DEL PROCESO
1	Servicio Mensajería Express Lima Metropolitana Y Callao	ONP	Coordinación de Gestión Documentaria	- Cargo - Acta de Notificación[2] - Correspondencia devuelta - Denuncia Policial

6.6.1. Descripción del Servicio

- El personal a cargo del recojo de documentos deberá estar contemplado en la relación presentada por el CONTRATISTA y autorizado por la ONP en la Fase Pre Operativa.

- Tanto el recojo como la devolución de la correspondencia y/o cargos, deberán realizarse en las oficinas de la ONP, según se detalla en el siguiente cuadro:

Cuadro Nº 04

OFICINAS DE ONP	DIRECCIÓN
Sede Central	Centro Cívico. Jr. Bolivia Nº 109 – Lima – Lima

- Durante la ejecución del servicio la ONP podrá incluir nuevas oficinas para el recojo de documentación y/o la actualización del Cuadro N° 04, las mismas que serán comunicadas formalmente.

- El recojo de la documentación será en días hábiles de lunes a viernes de 9:00 a 10:30 horas, el mismo que será controlado a través de un registro de asistencia.

- Podrá modificarse el horario de recojo de la correspondencia a solicitud de la ONP previa comunicación por correo electrónico y/o comunicación formal al contratista o a solicitud del contratista, debidamente sustentada para su aprobación de la ONP, a partir de la fecha indicada en la comunicación formal, la misma, que tendrá una anticipación mínima de 5 días calendario.

- La entrega de la correspondencia se emitirá en el Formato establecido en el Anexo Nº 02 en la que se registrará la cantidad de documentos o la correspondencia a entregar, con la firma y sello de Usuario de la ONP y del Contratista.

- Entregar la correspondencia al destinatario que se especifica en el mismo sobre.

- Devolver el respectivo documento cargo debidamente firmado por el destinatario o el Acta de Notificación o la constancia de la no entrega de la correspondencia, a la Supervisión del Contratista, o entrega de la denuncia policial mediante Carta por Mesa de Partes de la ONP.

[2] Ver Anexo Nº 04 – Formato de Acta de Notificación y Visita que debe ser suministrado por el Contratista.

- El cargo y/o Acta de Notificación deberán encontrarse en su aplicativo o la web del contratista, manteniendo la cantidad de folios que comprenden dichos documentos.

6.6.1.1. Características de la correspondencia

- El contenido de la correspondencia puede ser el siguiente: cartas, oficios, memorándums, informes, resoluciones, notificaciones, esquelas, pólizas, cheques, órdenes de pago u otros que serán definidos al momento de su entrega.

- El peso de cada envío es variable y será hasta un máximo de tres (3) kilogramos.

- El porcentaje de correspondencia que se encuentra en el rango de 0 a 1 Kg es el 99.3 %, de más de 1 Kg a 2 Kg es del 0.5 % y de más de 2Kg a 3 Kg es de 0.2%, cuyas cantidades referenciales se encuentran en el Anexo Nº 03 – en talsentido pueden variar de acuerdo a las necesidades de la ONP.

- La entrega de los envíos será en sobre cerrado acompañado con el documento cargo fuera del sobre, señalando nombre y dirección del destinatario.

6.6.1.2. Recojo, Traslado, Reparto y Notificación de los documentos

6.6.1.2.1. Para cada recojo que realice el contratista, la ONP entregará por correo electrónico en formato Excel un listado con la relación de la correspondencia a ser notificada, de acuerdo al Anexo Nº 02 Formato de Guía de Salida, a fin de que el contratista remita por correo electrónico y en formato Excel, antes del recojo físico, el número de guía asignado para dichas correspondencias.

6.6.1.2.2. Una vez efectuado el recojo de los documentos, el contratista se encargará de transportar, repartir y entregar dichos documentos a su destino, observando el control y el cuidado necesario, para su entrega óptima.

6.6.1.2.3. El Contratista deberá asegurar que los documentos de la ONP permanezcan en un ambiente seguro y separado del resto de los documentos de otros clientes, a fin de evitar su pérdida y/o que sus contenidos se hagan de conocimiento a terceras personas, ajenas al servicio o que reciba algún daño o deterioro del mismo, se deberá mantener las medidas de bioseguridad para evitar que los documentos sean expuestos a algún virus o bacteria, pudiendo perjudicar la salud de los clientes al momento de recibir su correspondencia.

6.6.1.2.4. El cargo (acto de notificación) debe estar completo y correcto, señalándose la fecha y hora de entrega, recabando el nombre y la firma de la persona a quien se notifica de acuerdo a lo establecido en la Ley N° 27444 contemplados en los artículos 21.3 y 21.4. En caso ésta se niegue a recibir la documentación o a firmar, se deberá registrar este hecho en el acta de notificación, teniéndose por bien notificado siempre y cuando se registre las características del domicilio donde se realizó la

notificación y se encuentre completamente llenado el Acta de Notificación. Ambos formatos (Cargo y Acta de Notificación) se encuentran contemplados en el Anexo Nº 04.

6.6.1.2.5. En el caso de no encontrar al administrado u otra persona en eldomicilio, el notificador deberá dejar constancia del acto colocando un aviso en dicho domicilio ("Aviso de Visita"), cuyo formato se encuentra establecido en el Anexo Nº 04, indicando la nueva fecha en que se hará efectiva la siguiente visita para la notificación. En caso, en esta segunda oportunidad, tampoco se pueda entregar la documentación, se deberá dejar constancia de ello en el "Acta de Notificación", cuya copia deberá ser anexada al sobre que contiene la documentación dejándola bajo puerta. Ambos formatos deberán ser llenados completamente y con información correcta.

6.6.1.2.6. El Contratista debe considerar que, para los casos de dirección errada o inubicable / desconocida, deberá realizar un segundo envío y será considerada como uno nuevo para efectos del reconocimiento de la facturación mensual, siempre que se cumpla con lo requerido en los presentes términos de referencia. Asimismo, la información de la dirección para el segundo envío será proporcionado por la ONP.

6.6.1.2.7. El Contratista deberá proporcionar a la ONP el acceso a su aplicativo o a la web para hacer seguimiento de la ubicación y situación del proceso de mensajería, esta deberá permitir la búsqueda por número de Guía de Salida (o la que haga sus veces) y destinario. Asimismo, deberá entregar una guía o manual de los términos usados en la web en la Fase Pre Operativa. La web debe contemplar los siguientes estados como mínimo de la labor de mensajería:

- Entregado[3]
- En proceso
- No entregado o No Distribuido
- Devuelto

6.6.1.2.8. El cargo de la correspondencia deberá ser escaneado y subido al aplicativo o la web del contratista, antes de la devolución física a la ONP, manteniendo la cantidad de folios que comprenden dichos documentos

6.6.1.2.9. La correspondencia entregada bajo puerta debe incluir el Acta de Notificación y el Aviso de Visita, los mismos que deberá ser escaneado y subido al aplicativo o la web del contratista, antes de la devolución física a la ONP, manteniendo la cantidad de folios que comprenden dichos documentos.

6.6.1.2.10. Sólo para la correspondencia que no haya sido recibida por el administrado, está deberá incluir el Acta de Notificación, donde expondrá los motivos por los cuales se negó a recibir la correspondencia, por lo que deberá ser escaneado y subido al aplicativo o la web del contratista, antes de la devolución física a la ONP, manteniendo la cantidad de folios que comprenden dichos documentos.

6.6.1.2.11. El Contratista deberá entregar a la ONP una Guía de devolución por correo electrónico en formato Excel y físico, que debe contemplar los campos establecidos en el Anexo Nº 05.

[3] Incluye las correspondencias entregadas bajo puerta

6.6.1.2.12. En los casos que no se encuentre disponible y actualizado el estado de los envíos realizados en el servicio consultando el Aplicativo o la Web, la ONP procederá a remitir un correo electrónico al Contratista solicitando el estado del envió, el mismo que dará atención en el día a dicha consulta, solo en los casos que las consultas sean efectuadas a partir de las 16:30 hrs del día, el contratista podrá remitir la información hasta el día siguiente antes del mediodía.

6.6.1.2.13. El procedimiento que debe seguir el contratista para la entrega de la correspondencia es el siguiente:

a) Recoger la correspondencia de acuerdo a los horarios establecidos en el numeral 6.6.1 debiendo estar el personal del contratista correctamente uniformado y portando la respectiva tarjeta de identificación.
b) Recoger la correspondencia, revisando la información establecida en el formato “Guía de Salida” con la correspondencia recibida y firmando y/o sellando en señal de conformidad.
c) Entregar la correspondencia según el Decreto Supremo Nº 004-2019-JUS que aprueba el Texto Único Ordenado de la Ley Nº 27444 - Ley del Procedimiento Administrativo General.
d) A la entrega de la correspondencia deberá obtener de parte del destinatario o quien recibe la documentación, la prueba fehaciente de la recepción, a través de los siguientes datos que deberá constar en el documento cargo enviado por la ONP:

d.1) Para personas naturales:
- Nombre y apellidos completos;
- Documento de identificación: Documento Nacional de Identificación (DNI), Carné de extranjería o pasaporte;
- Firma de la persona que recibe la documentación; y
- Fecha y hora de recepción.

d.2) Para personas jurídicas:
- Sello en el que figure el nombre de la empresa, institución o entidad;
- Firma y DNI de la persona que recibe la documentación, de ser el caso; y
- Fecha y hora de recepción.

6.6.1.2.14. El procedimiento que debe seguir el contratista en caso de que la correspondencia no pueda ser entregada al destinatario por razones no atribuibles es el siguiente:

a) En el horario establecido en el numeral 6.6.1, deberá devolver cada correspondencia no entregado adjuntando una guía (o lo que haga sus veces) o consignando en el mismo, la siguiente información:
- Fecha de entrega fallida
- Motivo: Dirección no existente, no permiten el acceso, destinatario errado, etc.;
- Características del lugar de entrega y/o número de suministro eléctrico, suministro de gas.
- Nombre y firma del mensajero

b) Para la devolución de los cargos y/o correspondencias el contratista entregará física y por correo electrónico una base en Excel con el Formato "Guía de Devolución" consignando obligatoriamente los campos detallados en el Anexo Nº 05.

c) La ONP podrá realizar el control y seguimiento del procedimiento verificando el cumplimiento; sin perjuicio de la aplicación de las penalidades respectivas.

6.6.1.2.15. En caso de pérdida de la correspondencia o de los documentos Cargo, el contratista deberá remitir la denuncia policial a la ONP la misma que debe contemplar los campos establecidos en Anexo Nº 06.

6.6.1.2.16. La denuncia policial deberá ser asentada máxima a los dos días calendario de sucedido el hecho y al subsiguiente día hábil, deberá presentar dicha denuncia a la Mesa de Partes de la ONP.

6.6.1.2.17. Señalamos, que una vez presentada la denuncia policial a ONP, no se aceptarán ampliaciones de la misma, en fechas posteriores de ocurridos los hechos.

6.6.1.2.18. El plazo establecido para la entrega de la correspondencia se encuentra contemplados en el Anexo Nº 01. El mismo que será computado a partir del día hábil siguiente de entregado la correspondencia para su notificación, y de caer en un día inhábil el plazo de la notificación, éste tendrá que ser notificado al día hábil siguiente; cuyo formato que permitirá dicho control será la Guía de Salida.

6.6.1.2.19. La entrega de la correspondencia se realizará únicamente en días decretados hábiles, de acuerdo a lo establecido, en el Texto Único Ordenado de la Ley Nº 27444 - Ley del Procedimiento Administrativo General.

6.6.1.2.20. La devolución de los cargos, actas de notificación y/o correspondencias deberán ser efectuadas al día siguiente de vencido el plazo de devolución, y de caer en un día inhábil, este tendrá que ser devuelto al día hábil siguiente; para un mejor entendimiento se pone como ejemplo:

Cuadro Nº 05

FORMATO	EJEMPLO 1		EJEMPLO 2	
	FECHA	ESTATUS	FECHA	ESTATUS
Guía de Salida	15/08/2022	Dentro del Plazo	15/08/2022	1 día fuera de plazo
Plazo de Entrega	2 días hábiles		2 días hábiles	
Vencimiento de plazo de entrega	17/08/2022		17/08/2022	
Plazo para devolución de cargo	3 días calendario		3 días calendario	
Guía de Devolución	22/08/2022		23/08/2022	

6.6.1.3. De los logotipos de la ONP

El Contratista ejecutará el servicio a nombre de la ONP quedando entendido que los formatos y demás materiales que cuenten con el logotipo de la ONP que utilice el contratista para sus operaciones son propiedad de la ONP y su uso deberá realizarse en estricto cumplimiento de las directivas que sobre el particular dicte la Entidad y circunscrito a las actividades del contratista en el servicio (la resolución que se encuentra vigente en la actualidad es la Resolución Jefatural N° 112-2020-JF/ONP).

Por ningún motivo, el Contratista podrá hacer uso de los formatos y demás material, para actividades distintas a las especificadas en el presente documento o las especificadas en el contrato.

La ONP entregará los modelos de los formatos y otros elementos requeridos para la operación del servicio brindado por el Contratista, de los Anexos Nº 04.

Al Cierre del Servicio el Contratista deberá haber entregado todos los formatos y demás materiales que cuenten con el logotipo de la ONP.

6.6.2. Obligaciones del Contratista

6.6.2.1. El contratista deberá contar con los recursos humanos necesarios, las unidades de transporte, los equipos y los materiales que sean necesarios para cumplir con los objetivos del servicio.

6.6.2.2. El personal técnico y operativo necesario para cumplir los turnos, la coordinación y la supervisión para que el servicio sea eficiente y oportuno.

6.6.2.3. El contratista es el responsable de supervisar el correcto cumplimiento de las funciones del personal asignado para la prestación del servicio.

6.6.2.4. El contratista se responsabiliza por los daños y perjuicios que pueda ocasionar el personal asignado a la ONP por la prestación defectuosa del servicio.

6.6.2.5. El Contratista deberá asumir las obligaciones que contraiga con su personal, sean laborales, personales o de cualquier otra naturaleza, estando eximida la Entidad de toda responsabilidad en caso de accidentes, daños, deceso de los trabajadores o de terceras personas que pudieran ocurrir durante la prestación del servicio. Estos riesgos deberán ser cubiertos íntegramente por las pólizas que el contratista está obligado a adquirir, las que deberán tener vigencia durante el plazo del contrato.

6.6.2.6. El contratista, si realizara un cambio de personal de recojo deberá informar la ONP con dos (2) días calendario de anticipación a fin de que pueda contar con la aprobación correspondiente de la ONP.

6.6.2.7. La ONP no tiene responsabilidad alguna por las obligaciones que contraiga el contratista con su personal.

6.6.2.8. El Contratista se compromete a cumplir y observar lo establecido en la Ley de Seguridad y Salud en el Trabajo (aprobado mediante Ley N° 29783) y su Reglamento, durante la ejecución de las prestaciones a su cargo; obligándose a implementar, dotar, proveer y/o suministrar a cada

uno de sus trabajadores los implementos de seguridad que corresponda de acuerdo al grado y/o nivel de riesgo que pueda evidenciarse en el desarrollo de cada componente propias de la presente contratación, así como garantizar la contratación de los respectivos seguros de acuerdo a la normatividad vigente.

6.6.2.9. El contratista deberá contar con un personal clave "Supervisor" que acredite formación académica como Bachiller universitario o título profesional técnico, según corresponda, asimismo, deberá acreditar capacitación de 16 horas lectivas en la Ley de Procedimiento Administrativo General – Ley N° 27444, y experiencia de cuatro (4) años como mínimo como supervisor o coordinador o jefe en mensajería y/o Courier y/o servicio postal o de Operaciones de mensajería, conforme a lo señalado en los requisitos de calificación, quien será el responsable de supervisar el correcto cumplimiento de las funciones del personal asignado para la prestación del servicio;, asimismo, el supervisor(a) brindará soporte necesario para la ejecución del servicio con quien la ONP realizará las coordinaciones, para lo cual el contratista deberá brindar al inicio del servicio los siguientes datos de contacto vigentes, como: número de contacto Celular/Fijo y Correo Electrónico.

6.6.2.10. En caso de presentarse algún cambio en el personal clave propuesto, el Contratista estará obligado a comunicar esta situación a la Oficina de Administración y presentar por mesa de partes de ONP, la propuesta del nuevo personal según el perfil solicitado o superior, a lo establecido en los términos de referencia, con una anticipaciónde dos (2) días calendario. ONP se pronunciará sobre el cambio de personal clave en el plazo de un (1) día calendario de recibida toda la documentación, previa aprobación del área usuaria, en caso de no haber respuesta de ONP, se dará por aprobado el cambio de personal clave.

6.6.3. Requisitos para la conformidad del servicio

6.6.3.1. Se considera que se ha completado la gestión de mensajería cuando se han realizado las siguientes actividades:

- El recojo de correspondencia en las Oficinas de la ONP.
- Se haya realizado la entrega de la correspondencia al destinatario.
- Se haya efectuado la devolución del Cargo, Acta de Notificación y/o Correspondencia devuelta, a la oficina de ONP de origen.
- En caso se haya presentado una pérdida o robo de la documentación la Denuncia Policial deberá ser devuelta de acuerdo a lo establecido en el punto 6.6.1.2.15, 6.6.1.2.16 y 6.6.1.2.17. Cabe señalar que, para el cómputo del pago, no será considerado las denuncias que registren pérdidadel cargo y/o correspondencia.

6.6.3.2. Para efectos del pago del servicio brindado, el contratista deberá presentar para cada periodo los siguientes entregables:

Cuadro Nº 06

N°	NOMBRE DEL ENTREGABLE	PLAZO DE ENTREGABLE	FORMA DE ENTREGA
1	Reporte de Liquidación Mensual de envíos realizados. Ver Anexo Nº 07	Dentro de los primeros quince (15) días calendarios del siguiente periodo de servicio	Será entregado mediante Carta a la Mesa de Partes, adjuntado el reporte en PDF y la Base de Datos en digital (Excel)
2	Reporte de las denuncias policiales por pérdida o robo. Ver Anexo Nº 06	Dentro de los primeros quince (15) días calendarios del siguiente periodo de servicio	Será entregado mediante Carta a la Mesa de Partes, adjuntado el reporte en PDF y la Base de Datos en digital(Excel)

De la revisión efectuada a los entregables, si se encontrará observaciones, el contratista tendrá que subsanar en un plazo máximo de siete (7) días calendarios de recibida la notificación de dichas observaciones, a fin de no afectar la conformidad del servicio. Cabe señalar, que la demora de la subsanación de las observaciones o subsanación fuera de plazo es atribuible a la aplicación de otras penalidades, para efectos del pago del periodo de dicho servicio.

7. PENALIDADES

7.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso, conforme al artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

7.2. OTRAS PENALIDADES

De acuerdo con el artículo 163 del Reglamento de la Ley de Contrataciones del Estado, se establecen penalidades distintas al retraso o mora en la ejecución de la prestación, las cuales son objetivas, razonables, congruentes y proporcionales con el objeto de la contratación.

N°	SUPUESTOS DE APLICACIÓN DE PENALIDAD			FORMA DE CÁLCULO		PROCEDIMIENTO
	RUBRO	SUMILLA	CONCEPTO			
1	Calidad	Deterioro	Por deterioro parcial o total de un documento por razones atribuibles al Contratista. Se define por deterioro parcial o una inadecuada preservación, cuando el elemento bajo custodia durante el periodo de ejecución del servicio, ha sido, entre otros: manchado, enmendado, roto, doblado, humedecido o contiene sujetadores de papel oxidados, rotos o incompletos o carece de ellos, que afectan el contenido parcial del documento, que no permita leer la información fehacientemente.Se define por deterioro total, cuando el elemento bajo custodia durante el periodode ejecución del servicio ha sido, entre otros: mojado, quemado o roto en el extremo que la información no sea legible y que afectan el contenido total del documento. De producirse el deterioro parcial o total de un documento producto de fenómenos naturales o de terceros: Inundaciones, terremoto, temblor, maremoto, salida del mar, vandalismo, terrorismo, huelga, motín, conmoción civil no serán atribuibles al contratista.	0.2%	UIT por documento detectado	Se describe en el numeral 7.2.1 Procedimiento de aplicación de penalidad.
2	Calidad	Procedimientos	Por el incumplimiento de los siguientes procedimientos: a) El cargo (acto de notificación) debe estar completo y correcto, señalándose la fecha y hora de entrega, recabando el nombre y la firma de la persona a quien se notifica de acuerdo a lo establecido en la Ley N° 27444 contemplados en los artículos 21.3 y 21.4. En caso ésta se niegue a recibir la documentación o a firmar, se deberá registrar este hecho en el acta de notificación, teniéndose por bien notificado siempre y cuando se registre las características del domicilio donde se realizó la notificación y se encuentre completamente llenado el Acta de Notificación. Ambos formatos (Cargo y Acta de Notificación) se encuentran contemplados en el Anexo Nº 04. b) En el caso de no encontrar al administrado u otra persona en el domicilio, el notificador deberá dejar constancia del acto colocando un aviso en dicho domicilio (“Aviso de Visita”), cuyo formato se encuentra establecido en el Anexo Nº 04, indicando la nueva fecha en que se hará efectiva la siguiente visita para la notificación. En caso, en esta segunda oportunidad, tampoco se pueda entregar la documentación, se deberá dejar constancia de ello en el “Acta de Notificación”, cuya copia deberá ser anexada al sobre que contiene la documentación dejándola bajo puerta. Ambos formatos deberán ser llenados completamente y con información correcta.	0.2%	de UIT por cada documento detectado.	Se describe en el numeral 7.2.1 Procedimiento de aplicación de penalidad.

N°	SUPUESTOS DE APLICACIÓN DE PENALIDAD			FORMA DE CÁLCULO		PROCEDIMIENTO
	RUBRO	SUMILLA	CONCEPTO			
			c) El cargo y/o Acta de Notificación debe ser escaneado y subido al aplicativo o la web del contratista, antes de la devolución física a la ONP, manteniendo la cantidad de folios que comprenden dichos documentos. d) En los casos que no se encuentre disponible y actualizado el estado de los envíos realizados en el servicio consultando el Aplicativo o la Web, la ONP procederá a remitir un correo electrónico al Contratista solicitando el estado del envió, el mismo que dará atención en el día a dicha consulta, solo en los casos que las consultas sean efectuadas a partir de las 16:30 hrs del día, el contratista podrá remitir la información hasta el día siguiente antes del mediodía.			
3	Calidad	Entregables	Por no presentar cualquiera de los entregables señalados dentro de los plazos establecidos en los Términos de Referencia o por presentar los entregables incompletos, el cual, se tomará como un entregable no presentado.	0.5%	de UIT por cada día de atraso	Se describe en el numeral 7.2.1 Procedimiento de aplicación de penalidad.
4	Calidad	Entregables	Por presentar cualquiera de los entregables señalados en los presentes Términos de Referencia con inconsistencia o errores, sin perjuicio de la subsanación correspondiente. Se entiende por inconsistencia a cualquier información incorrecta y/o inexacta relacionada a: cantidades, plazos, fechas, ubicaciones, actividades o datos.	1.5%	de UIT por cada entregable por ocurrencia.	Se describe en el numeral 7.2.1 Procedimiento de aplicación de penalidad.
5	Calidad	Destino errado	Si el contratista entrega la correspondencia en un lugar diferente al domicilio del destinatario.	0.4%	de UIT, por cada ocurrencia detectado.	Se describe en el numeral 7.2.1 Procedimiento de aplicación de penalidad.
6	Calidad	Quejas	Si posterior a la labor de mensajería, la Institución toma conocimiento de quejas, reclamos o denuncias por parte de los destinatarios sobre el proceso de mensajería realizado atribuibles al contratista.	0.5%	de UIT, por cada ocurrencia detectado.	Se describe en el numeral 7.2.1 Procedimiento de aplicación de penalidad.
7	Condición del Servicio	Denuncia Oportuna	Por no asentar la Denuncia Policial por pérdida o robo de la correspondencia, dentro de los dos (2) días calendario del día siguiente de producido el hecho.	0.1%	UIT por documento y por cada día (sobre o cargo) detectado	Se describe en el numeral 7.2.1 Procedimiento de aplicación de penalidad.
8	Condición del Servicio	Presentación de la Denuncia Policial	Por la no remisión de la Denuncia Policial por pérdida o robo de la correspondencia, dentro de los tres (3) días calendario de producido el hecho.	0.1%	UIT por documento y por cada día (sobre o cargo) detectado	Se describe en el numeral 7.2.1 Procedimiento de aplicación de penalidad.

N°	SUPUESTOS DE APLICACIÓN DE PENALIDAD			FORMA DE CÁLCULO		PROCEDIMIENTO
	RUBRO	SUMILLA	CONCEPTO			
9	Personal	Horario	Si el Contratista no se presentara a recoger la correspondencia o no se presentará en el horario programado para el recojo. Se tomará asistencia en el ambiente establecido la Unidad Funcional de Gestión Documentaria de la ONP, teniendo en consideración en lo establecido en el numeral 6.6.1	2.5%	de UIT por cada día detectado	Se describe en el numeral 7.2.1 Procedimiento de aplicación de penalidad.
10	Personal	Violación de Correspondencia	Si el personal del contratista incurre en el delito de violación de correspondencia, conforme a la denuncia policial que interponga el respectivo destinatario.	1%	de UIT por cada evento denunciado	Se describe en el numeral 7.2.1 Procedimiento de aplicación de penalidad.
11	Políticas de Seguridad	Incumplimiento de políticas	Por el incumplimiento de la presentación de la “Declaración Jurada- Cumplimiento de políticas de seguridad de la información” y “Compromiso de Confidencialidad”, dentro de la Fase Pre Operativa. Esta penalidad tiene como base el documento “Políticas de Seguridad de ONP” (Directiva DIR-02/01 Lineamientos de Seguridad de la Información)	0.5%	de UIT por cada día detectado	Se describe en el numeral 7.2.1 Procedimiento de aplicación de penalidad.

7.2.1. Procedimiento de aplicación de penalidad

7.2.1.1. El procedimiento para la aplicación de las otras penalidades es el siguiente:

a. El área usuaria comunicará por escrito al contratista sobre las situaciones pasibles de penalidad indicando la causal, base legal y el plazo.
b. El contratista tendrá hasta siete (7) días calendario contados a partir del día siguiente de recibida la comunicación, para efectuar el descargo respectivo.
c. Recibido el descargo del contratista o no habiendo recibido respuesta alguna dentro del plazo concedido, el área usuaria procede a su evaluación y determina la confirmación o no, de la aplicación de la penalidad y se procederá a comunicar al contratista.
d. Paralelamente a ello, el área usuaria informa a la OAD para que proceda al cobro de la penalidad aplicada.
e. La/El Ejecutiva/o de Logística remite el importe de la penalidad a cobrar a la/el Ejecutiva/o de Tesorería, para este último, bajo responsabilidad, proceda al cobro de la penalidad aplicada.
f. En caso de que no sea posible el cobro administrativo de la penalidad, la/el Ejecutiva/o de Tesorería comunica este hecho a la/el Ejecutiva/o de Logística para las acciones correspondientes.
g. La aplicación de la penalidad opera sin perjuicio del cumplimiento, corrección o subsanación del hecho que motivó la penalidad, por parte del Contratista.

7.2.1.2. Tanto las penalidades por mora como las otras penalidades contempladas podrán ser aplicadas en cualquier momento durante la vigencia del contrato.

7.2.1.3. Estas penalidades se deducen de los pagos a cuenta, de las valorizaciones, del pago final o en la liquidación final, según corresponda; o si fuera necesario, se cobra del monto resultante de la ejecución de la garantía de fiel cumplimiento.

7.2.1.4. En virtud a lo dispuesto por los artículos 161, 162 y 163 del Reglamento de la Ley de Contrataciones del Estado, Los dos tipos de penalidades pueden alcanzar cada una un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, o de ser el caso, del ítem que debió ejecutarse, por lo que la ONP no aplicará penalidades por mora y otras penalidades más allá de dicho porcentaje, en cuya situación, la ONP podrá resolver el contrato por incumplimiento, en aplicación a lo dispuesto en los citados artículos.

7.2.1.5. Se precisa que, en caso de existir alguna controversia que se pudiera generar por la aplicación de alguna penalidad, el Contratista podrá someter arbitraje de acuerdo al artículo 223 del Reglamento de la Ley de Contrataciones del Estado.

8. SEGUROS

El CONTRATISTA deberá presentar a la suscripción del contrato las siguientes pólizas de seguro y es responsable de mantener su vigencia durante el periodo del Contrato, a su total y único costo las pólizas y coberturas que como mínimo se indican en el presente numeral, las cuales deberán ser contratadas con una aseguradora debidamente autorizada por la SBS, asimismo, para suscripción del contrato, EL CONTRATISTA deberá presentar la factura que demuestre el pago total de la prima correspondiente, o en su defecto, un Convenio de Pago válidamente emitido por la Compañía de Seguros correspondiente con las facturas por las cuotas vencidas a la fecha de presentación de los documentos.

El CONTRATISTA deberá notificar a la ONP en caso se prevé renovar, cancelar o modificar algunas de las condiciones de los seguros con una anticipación no menor a quince (15) días calendarios.

Las pólizas que como mínimo deberán ser contratadas por el CONTRATISTA serán las siguientes.

i) SEGURO DESHONESTIDAD

Ubicación del Riesgo
Oficina de la ONP

Materia del Seguro
Personal del CONTRATISTA que recogerá correspondencia en las instalaciones de la ONP.

Nº de Asegurados
Debe declararse el número total de colaboradores que el CONTRATISTA dispondrá para el recojo de correspondencia en el ambiente establecido por el equipo de trabajo de Gestión Documentaria de la ONP.

Suma Asegurada
No menor a US$ 20, 000 (Veinte Mil) dólares americanos por evento y US$ 100, 000 (Cien mil Dólares) dólares americanos en el agregado anual.

Cobertura
Deshonestidad de Empleados

Deducible
Si se incluye un Deducible Porcentual respecto del monto del siniestro o monto indemnizable, esto no deberá ser mayor al 10%. Adicionalmente si se incluye un Deducible mínimo este no deberá ser mayor a US$ 1,000 (mil) dólares americanos.

Cláusula Especial
Se debe considerar Cláusula de Cesión de Derechos Indemnizatorios a favor de la Entidad o considerar a la Entidad como Asegurado Adicional.

ii) SEGURO DE RESPONSABILIDAD CIVIL

Ubicación del Riesgo
Oficina de la ONP

Coberturas

- Responsabilidad Civil Extracontractual
- Responsabilidad Civil Patronal

Suma Asegurada
No menor a US$ 30,000 (Treinta Mil Dólares) dólares americanos por evento y US$ 100,000 (Cien mil Dólares) dólares americanos en el agregado anual.

Deducible
Si se incluye un Deducible Porcentual del monto del siniestro o monto indemnizable, este no deberá ser mayor al 10%. Adicionalmente si se incluye un Deducible Mínimo este no deberá ser mayor a US$ 1,000 (Mil dólares americanos).

Condición Especial

Se debe considerar a la Entidad como Asegurado Adicional dentro de la póliza, pero manteniendo a su vez su calidad de tercero en caso de daños que le sean causados directamente por el contratante del seguro.

iii) EL CONTRATISTA SE ENCUENTRA OBLIGADO A CONTRATAR LOS SEGUROS DE LEY, COMO SON:

a) Seguro de Vida Ley.
b) Seguro Complementario por Trabajo de Riesgo.

ONP podrá exigir los Certificados o Constancias de los Seguros mencionados para autorizar el ingreso del personal propuesto del Contratista a los Locales de ONP, para el cumplimiento del presente servicio.

Las Pólizas deben tener la vigencia del servicio propuesto y de vencer su anualidad, el Contratista está obligado a renovarlas y alcanzar copia de las mismas con su respectivo pago y comprobante, con una anticipación de 15 días calendario.

9. PLAZOS

9.1. Plazo Pre Operativa: El inicio de la fase Pre Operativa será a partir del día siguiente de la suscripción del contrato por un plazo máximo de 10 días calendario.

9.2. Plazo de Ejecución del Servicio: El plazo de ejecución del servicio se iniciará al día siguiente de la culminación de la fase Pre Operativa del Servicio Mensajería Express Lima Metropolitana y Callao (suscripción del Acta Pre Operativa), por un periodo de 1,096 días calendario o hasta agotar el monto contractual, lo que ocurra primero.

10. SISTEMA DE CONTRATACIÓN

El sistema de contratación es a precios unitarios.

11. FORMALIZACIÓN DE LOS SERVICIOS

El servicio de mensajería será formalizado mediante contrato, se deberá adjuntar la estructura de costos correspondiente.

A la firma del contrato, el Contratista como mínimo deberá presentar al equipo de trabajo de Logística – ONP, la estructura de costos del Servicio. Esta estructura deberá contener como mínimo el detalle por cada producto, según Anexo N° 08: Estructura Mínima de Costos.

El precio debe incluir todos los tributos, seguros, transporte, inspecciones, pruebas y de ser el caso, los costos laborales conforme a la legislación vigente, así como otro concepto que pueda tener incidencia del servicio contratado.

12. ENTREGABLES DEL SERVICIO

Los entregables deberán presentarse dentro de los quince (15) primeros días calendario del siguiente mes de finalizado cada periodo de servicio (cada periodo de servicio será de 30 días calendario).

Los entregables deberán ser presentado vía mesa de partes virtual mesadepartes@onp.gob.pe de la entidad o a través de la Mesa de Partes de la Oficina de Normalización Previsional ubicada en Jr. Bolivia N° 109 - Cercado de Lima, salvo de disponerse otro medio para la presentación del Entregable, éste será comunicado en su oportunidad al contratista.

13. CONFORMIDAD DE SERVICIO

La conformidad del servicio será emitida por la/el Coordinador/a de la Unidad Funcional de Gestión Documentaria.

Solo para la conformidad del último periodo el CONTRATISTA, deberá entregar todos los documentos, asegurando saldo cero de pendientes del proceso, entre ellos:entrega física de todos los documentos, cargos y/o correspondencias procesados y recibidos hasta el último día de las operaciones.

Por tanto, sólo se podrá brindar conformidad final (Anexo N° 11 y N° 12), cuando el Contratista haya efectuadoel retorno del último cargo a las oficinas de ONP (Lima Metropolitana y Callao), para lo cual contará con un plazo de 15 días calendario contabilizados a partir del día siguiente de finalizada la Fase Operativa, según corresponda.

14. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en pagos periódicos mensuales, precisándose que el pago se efectuará de acuerdo a los reportes de liquidación contemplados en los puntos 6.6.3 de los términos de referencia, según corresponda; considerando el precio unitario ofertado por el contratista, durante la vigencia del contrato.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente información:

a) Para los pagos del 1 al periodo 35

- Reporte de la Liquidación Mensual de envíos realizados por el contratista (Anexo N° 7), el citado reporte será presentado por Mesa de Partes virtual o física de la ONP.
- Reporte Mensual de las denuncias policiales por pérdida o robo (Anexo N° 6), el citado reporte será presentado por Mesa de Partes virtual o física de la ONP.
- Conformidad de servicio emitida por el/la Coordinador(a) de la Unidad Funcional de Gestión Documentaria.
- Comprobante de pago.

b) Para el pago del periodo 36

- Reporte de la Liquidación Mensual de envíos realizados por el contratista (Anexo N° 7), el citado reporte será presentado por Mesa de Partes virtual o física de la ONP.
- Reporte Mensual de las denuncias policiales por pérdida o robo (Anexo N° 6), el citado reporte será presentado por Mesa de Partes virtual o física de la ONP.
- Conformidad de servicio emitida la por el/la Coordinador(a) de la Unidad Funcional de Gestión Documentaria.
- Comprobante de pago.
- Reporte Final del contratista (Anexo N° 11 y 12),el citado reporte será presentado por Mesa de Partes virtual o física de la ONP, el mismo que debe contener como mínimo lo siguiente:

    1. Resumen de las cantidades mensuales, con los respectivos estados durante la vigencia del contrato.
    2. Estatus de la facturación durante la vigencia del contrato.

La Entidad paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

15. RESPONSABILIDAD DEL CONTRATISTA

La conformidad del servicio por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 40 de la Ley de Contrataciones del Estado y 146 de su Reglamento.

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos del servicio ofertado, con un plazo máximo de un (1) año, contado a partir de la conformidad.

16. FÓRMULA DE REAJUSTE

Para el presente servicio no se considerarán fórmulas de reajuste.

17. CONFIDENCIALIDAD

El proveedor por contratar se compromete a no revelar, comentar, suministrar o transferir de cualquier forma a terceros, cualquier información estrictamente confidencial que hubiese recibido directa o indirectamente de la ONP o que hubiese sido generada como parte del servicio. El incumplimiento de esta obligación será causal de resolución del contrato y de ser el caso la ONP se reserva el derecho de interponer las acciones legales que correspondan, en caso de que el proveedor incumpla esta condición, aún después de ejecutado el servicio.

18. MEDIDAS DE SEGURIDAD SANITARIA EN LA PRESTACIÓN DEL SERVICIO

- Para la ejecución del servicio, el contratista deberá debe tener en cuenta la normativa para la vigilancia, prevención y control de COVID-19 dispuesta por el Estado, así como lo indicado en el Anexo Nº 09 - Plan para la Vigilancia, prevención y control del COVID-19 en el trabajo de la Oficina de Normalización Previsional:

    - Presentar la documentación para el ingreso de proveedores a las instalaciones en el contexto de la COVID-19, descrito en el ***"Anexo del Plan para la Vigilancia, Prevención y Control de la COVID-19 en el Trabajo de la ONP".***

19. POLÍTICA ANTISOBORNO

La ONP, mediante Resolución Jefatural N° 016-2022-ONP/JF, aprobó la Política Antisoborno y Objetivos del Sistema de Gestión Antisoborno, la cual está disponible en el siguiente enlace: https://www.gob.pe/institucion/onp/normas-legales/2721514-016-2022-onp-jf".

20. SEGURIDAD DE LA INFORMACIÓN

En el marco de la Directiva DIR-02/01 Lineamientos de Seguridad de la Información, el Contratista deberá cumplir con los lineamientos y normativa vigente.

El personal del Contratista deberá suscribir el ***Compromiso de Confidencialidad*** *y* ***Declaración Jurada de Cumplimiento de Política de Seguridad de la Información***, contemplados en dicha Directiva, contemplados en dicha Directiva, en la etapa Pre Operativa.

El contratista será responsable del deterioro, pérdida o sustracción de los documentos mientras estos se encuentren en su poder o bajo su responsabilidad.

Los archivos electrónicos generados (imágenes, base de datos, archivos textos y otros) en cada una de las etapas, por ningún motivo podrán ser divulgados ni física ni electrónicamente, considerándose la divulgación parcial o total del producto del presente servicio como delito contra la propiedad, pasible de establecer las demandas que se consideren necesarias contra la empresa contratada y ante las instituciones competentes.

El Contratista deberá reportar al Oficial de Seguridad de la Información de la ONP, los incidentes de seguridad de la Información que afecten a la confidencialidad, integridad o disponibilidad de la información del Servicio, en un plazo no mayor de 2 horas de ocurrido el incidente.

El uso del correo electrónico debe ser exclusivo para fines laborales.

21. ANEXOS

- Anexo Nº 01 - Cuadro de Términos de la Distancia para el Servicio Mensajería Express Lima Metropolitana Y Callao
- Anexo Nº 02 - Formato de Guía de Salida
- Anexo Nº 03 - Cantidades Estimadas de los Productos
- Anexo Nº 04 - Formato de Acta de Notificación, Aviso de Visita y Cargo
- Anexo Nº 05 - Formato de Guía de Devolución
- Anexo Nº 06 – Formato de Denuncia Policial por Pérdida o Robo
- Anexo Nº 07 - Formato de Reporte Mensual
- Anexo Nº 08 - Estructura Mínima de Costos
- Anexo Nº 09 - Plan para la Vigilancia, prevención y control del COVID-19 en el trabajo.
- Anexo Nº 10 - Directiva DIR-02/01 Lineamientos de Seguridad de la Información.
- Anexo N° 11 – Reporte Final de Mensajería.
- Anexo N° 12 – Reporte Final de denuncias policiales por pérdida o robo.

Anexo Nº 01 Cuadro de Términos de la Distancia para el Servicio Mensajería Express Lima Metropolitana y Callao, destinos descritos en el presente Anexo con un plazo de dos (2) días hábiles de entrega y tres (3) días calendario de devolución del cargo respectivo.

TIPO DE ENVIO	DEPARTAMENTO	PROVINCIA	DISTRITO	PLAZO DÍA HÁBILES	PLAZO DE DEVOLUCION DEL CARGO, ACTA DE NOTIFICACIÓN O CORRESPONDENCIA DÍAS CALENDARIO
LOCAL	LIMA	LIMA	ANCON	2	**3**
LOCAL	LIMA	LIMA	ATE	2	**3**
LOCAL	LIMA	LIMA	BARRANCO	2	**3**
LOCAL	LIMA	LIMA	BREÑA	2	**3**
LOCAL	LIMA	LIMA	CARABAYLLO	2	**3**
LOCAL	LIMA	LIMA	CHACLACAYO	2	**3**
LOCAL	LIMA	LIMA	CHORRILLOS	2	**3**
LOCAL	LIMA	LIMA	CHOSICA (LURIGANCHO)	2	**3**
LOCAL	LIMA	LIMA	CIENEGUILLA	2	**3**
LOCAL	LIMA	LIMA	COMAS (LIM)	2	**3**
LOCAL	LIMA	LIMA	EL AGUSTINO	2	**3**
LOCAL	LIMA	LIMA	INDEPENDENCIA	2	**3**
LOCAL	LIMA	LIMA	JESUS MARIA	2	**3**
LOCAL	LIMA	LIMA	LA MOLINA	2	**3**
LOCAL	LIMA	LIMA	LA VICTORIA	2	**3**
LOCAL	LIMA	LIMA	LIMA	2	**3**
LOCAL	LIMA	LIMA	LINCE	2	**3**
LOCAL	LIMA	LIMA	LOS OLIVOS	2	**3**
LOCAL	LIMA	LIMA	LURIN	2	**3**
LOCAL	LIMA	LIMA	MAGDALENA DEL MAR	2	**3**
LOCAL	LIMA	LIMA	MIRAFLORES	2	**3**
LOCAL	LIMA	LIMA	PACHACAMAC	2	**3**
LOCAL	LIMA	LIMA	PUCUSANA	2	**3**
LOCAL	LIMA	LIMA	PUEBLO LIBRE (MAGDALENA VIEJA)	2	**3**
LOCAL	LIMA	LIMA	PUENTE PIEDRA	2	**3**
LOCAL	LIMA	LIMA	PUNTA HERMOSA	2	**3**
LOCAL	LIMA	LIMA	PUNTA NEGRA	2	**3**
LOCAL	LIMA	LIMA	RIMAC	2	**3**
LOCAL	LIMA	LIMA	SAN BARTOLO	2	**3**
LOCAL	LIMA	LIMA	SAN BORJA	2	**3**
LOCAL	LIMA	LIMA	SAN ISIDRO	2	**3**
LOCAL	LIMA	LIMA	SAN JUAN DE LURIGANCHO	2	**3**
LOCAL	LIMA	LIMA	SAN JUAN DE MIRAFLORES	2	**3**
LOCAL	LIMA	LIMA	SAN LUIS	2	**3**
LOCAL	LIMA	LIMA	SAN MARTIN DE PORRES	2	**3**
LOCAL	LIMA	LIMA	SAN MIGUEL	2	**3**
LOCAL	LIMA	LIMA	SANTA ANITA	2	**3**
LOCAL	LIMA	LIMA	SANTA MARIA DEL MAR	2	**3**
LOCAL	LIMA	LIMA	SANTA ROSA	2	**3**
LOCAL	LIMA	LIMA	SANTIAGO DE SURCO	2	**3**
LOCAL	LIMA	LIMA	SURQUILLO	2	**3**
LOCAL	LIMA	LIMA	VILLA EL SALVADOR	2	**3**
LOCAL	LIMA	LIMA	VILLA MARIA DEL TRIUNFO	2	**3**

LOCAL	CALLAO	CALLAO	BELLAVISTA	2	**3**
LOCAL	CALLAO	CALLAO	CALLAO	2	**3**
LOCAL	CALLAO	CALLAO	CARMEN DE LA LEGUA REYNOSO	2	**3**
LOCAL	CALLAO	CALLAO	LA PERLA	2	**3**
LOCAL	CALLAO	CALLAO	LA PUNTA	2	**3**
LOCAL	CALLAO	CALLAO	MI PERU	2	**3**
LOCAL	CALLAO	CALLAO	VENTANILLA	2	**3**

Nota: El incumplimiento de estos plazos será aplicado de acuerdo a lo establecido en el punto 7.1 de los Términos de Referencia.

Anexo Nº 02: **Formato de Guía de Salida**

FORMATO DE GUIA DE SALIDA

ORD	CLASIRCACIÓN(PREVISIONAL/ADMINISTRATIVO)	RESPONSABLE DEL AREA	AREA USUARIA	NUMERO DE DOCUMENTO	DESTINATARIO	DIRECCION	DEPARTAMENTO	PROVINCIA	DISTRITO	FECHA DE ENVIO	TIPO DE ENVIO	TIPO DE DOCUMENTO	NUMERO DE GUIA	CORRELATIVO
1														
2														
3														
4														
5														

Leyenda:
Tipo de Envío: Local
Tipo de Documento: Notificación, Resolución, Oficio, Constancia, Carta, otros.
Fecha de Envío: Fecha de Entrega a Courier

Anexo Nº 03: Cantidades Estimadas de los Envíos

	SERVICIO	DESTINO	CANTIDAD MENSUAL -2023 (REFERENCIAL)	CANTIDAD MENSUAL - 2024 (REFERENCIAL)	CANTIDAD MENSUAL -2025 (REFERENCIAL)
	Servicio Mensajería Express Lima Metropolitana Y Callao	LIMA METROPOLITANA Y CALLAO	8795	8199	8323
		TOTAL	8,795	8,199	8,323

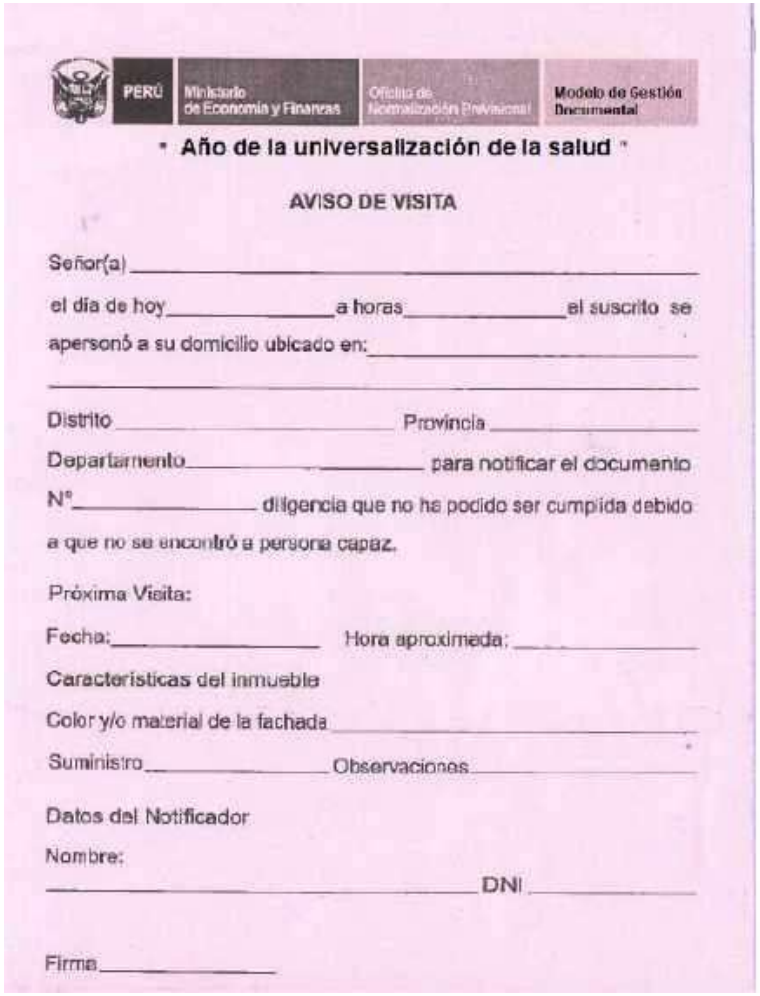
.

	SERVICIO	DESTINO	CANTIDAD ANUAL-2023 (REFERENCIAL)	CANTIDAD ANUAL-2024 (REFERENCIAL)	CANTIDAD ANUAL-2025 (REFERENCIAL)	ESTIMADA (CANTIDAD TOTAL DEL SERVICIO)	PRECIO UNITARIO	PRECIO TOTAL
	Servicio Mensajería Express Lima Metropolitana Y Callao	LIMA METROPOLITANA Y CALLAO	105538	98386	99873	303797		
		TOTAL	105,538	98,386	99,873	303,797		

Nota: La frecuencia de los envíos locales varia todos los meses de acuerdo a la necesidad del servicio, por ello, dichas cantidades son referenciales.

Anexo Nº 04: Formato de Acta de Notificación, Aviso de Visita y Cargo

- **Formato: Aviso de Visita (Autocopiativo) – Tamaño A5, será suministrado por el Contratista.**



PERÚ | Ministerio de Economía y Finanzas | Oficina de Normalización Previsional | Modelo de Gestión Documental

" Año de la universalización de la salud "

AVISO DE VISITA

Señor(a) _____

el día de hoy _____ a horas _____ el suscrito se apersonó a su domicilio ubicado en: _____

_____

Distrito _____ Provincia _____

Departamento _____ para notificar el documento N° _____ diligencia que no ha podido ser cumplida debido a que no se encontró a persona capaz.

Próxima Visita:

Fecha: _____ Hora aproximada: _____

Características del inmueble

Color y/o material de la fachada _____

Suministro _____ Observaciones _____

Datos del Notificador

Nombre:

_____ DNI _____

Firma _____

PERÚ | Ministerio de Economía y Finanzas | Oficina de Normalización Previsional | Modelo de Gestión Documental

" Año de la universalización de la salud "

AVISO DE VISITA

Señor(a) _____

el día de hoy _____ a horas _____ el suscrito se apersonó a su domicilio ubicado en: _____

_____

Distrito _____ Provincia _____

Departamento _____ para notificar el documento N° _____ diligencia que no ha podido ser cumplida debido a que no se encontró a persona capaz.

Próxima Visita:

Fecha: _____ Hora aproximada: _____

Características del inmueble

Color y/o material de la fachada _____

Suministro _____ Observaciones _____

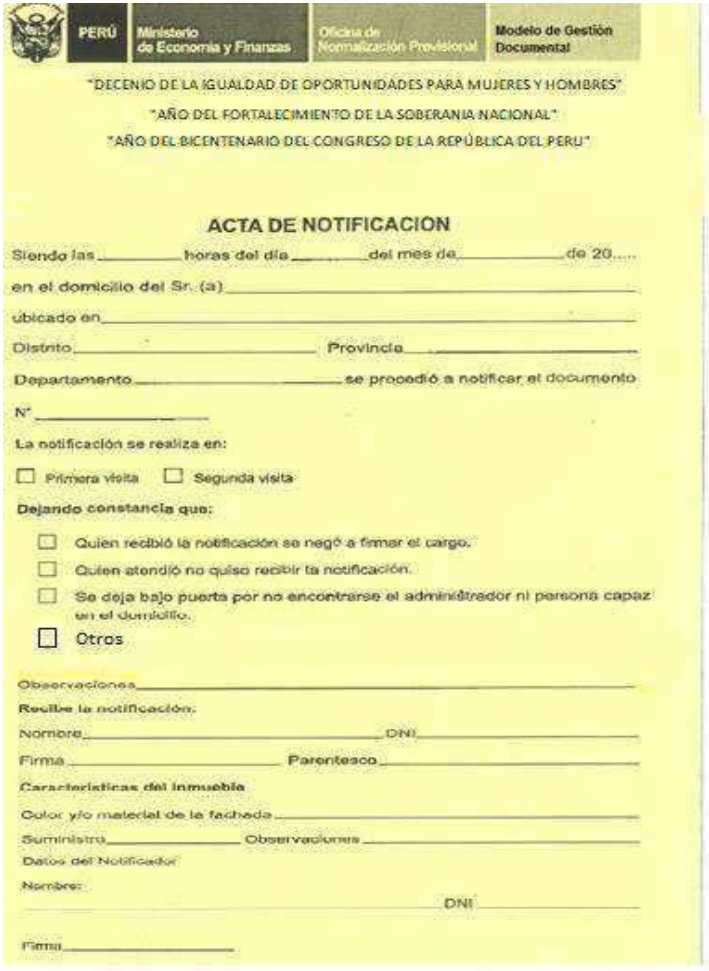
Datos del Notificador

Nombre:

_____ DNI _____

Firma _____

- **Formato: Acta de Notificación (Autocopiativo) – Tamaño A5, será suministrado por el Contratista. (se cambiará anualmente el nombre oficial del año)**



PERÚ | Ministerio de Economía y Finanzas | Oficina de Normalización Previsional | Modelo de Gestión Documental

"DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES"
"AÑO DEL FORTALECIMIENTO DE LA SOBERANIA NACIONAL"
"AÑO DEL BICENTENARIO DEL CONGRESO DE LA REPÚBLICA DEL PERU"

ACTA DE NOTIFICACION

Siendo las _____ horas del día _____ del mes de _____ de 20.....
en el domicilio del Sr. (a) _____
ubicado en _____
Distrito _____ Provincia _____
Departamento _____ se procedió a notificar el documento
N° _____
La notificación se realiza en:
☐ Primera visita ☐ Segunda visita
Dejando constancia que:
☐ Quien recibió la notificación se negó a firmar el cargo.
☐ Quien atendió no quiso recibir la notificación.
☐ Se deja bajo puerta por no encontrarse el administrador ni persona capaz en el domicilio.
☐ Otros

Observaciones _____
Recibe la notificación:
Nombre _____ DNI _____
Firma _____ Parentesco _____
Características del inmueble
Color y/o material de la fachada _____
Suministro _____ Observaciones _____
Datos del Notificador
Nombre:
_____ DNI _____
Firma _____

PERÚ | Ministerio de Economía y Finanzas | Oficina de Normalización Previsional | Modelo de Gestión Documental

"DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES"
"AÑO DEL FORTALECIMIENTO DE LA SOBERANIA NACIONAL"
"AÑO DEL BICENTENARIO DEL CONGRESO DE LA REPÚBLICA DEL PERU"

ACTA DE NOTIFICACIÓN

Siendo las _____ horas del día _____ del mes de _____ de 20.....
en el domicilio del Sr. (a) _____
ubicado en _____
Distrito _____ Provincia _____
Departamento _____ se procedió a notificar el documento
N° _____
La notificación se realiza en:
☐ Primera visita ☐ Segunda visita
Dejando constancia que:
☐ Quien recibió la notificación se negó a firmar el cargo.
☐ Quien atendió no quiso recibir la notificación.
☐ Se deja bajo puerta por no encontrarse el administrador ni persona capaz en el domicilio.
☐ Otros

Observaciones _____
Recibe la notificación:
Nombre _____ DNI _____
Firma _____ Parentesco _____
Características del inmueble
Color y/o material de la fachada _____
Suministro _____ Observaciones _____
Datos del Notificador
Nombre:
_____ DNI _____
Firma _____

- **Formato: Cargo – Tamaño A5, será suministrado por la ONP.**

OFICINA DE NORMALIZACION PREVISIONAL
CARGO DE ENTREGA DE NOTIFICACION

Tipo de Documento

Nro. de Documento **Ley**
Descripción

Nro. Resolución

Fecha de Envio

Expediente
Cuenta de Pensión

Nombre
Dirección

Distrito
Provincia
Departamento

Recibido por _____

Documento de Identidad _____

Parentesco _____

Fecha de Entrega _____ **FIRMA** ____ _____

Hora de Entrega _____

MOTIVO DE DEVOLUCION

☐ Dirección errada ☐ Se mudo ☐ Ausente
☐ Rechazado ☐ Desconocido ☐ Otros

N DOCUMENTO
Nro Documento

EXPEDIENTE
Nro de Expediente

Anexo Nº 05: Formato de Guía de Devolución

FORMATO DE GUIA DE DEVOLUCION

ITEM	CLASIFICACIÓN (PREVISIONAL/ADMINISTRATIVO)	RESPONSABLE DEL AREA	AREA USUARIA	NUMERO DE DOCUMENTO	DESTINATARIO	DIRECCION	DEPARTAMENTO	PROVINCIA	DISTRITO	FECHA DE ENVIO	TIPO DE ENVIO	TIPO DE DOCUMENTO	PESO	N° DE GUIA	CORRELATIVO	FECHA DE 1RA VISITA	FECHA DE ENTREGA AL DESTINATARIO	FECHA DE DEVOLUCION DEL DOCUMENTO CARGO (*)	GUIA DEV.	ESTADO DE DOCUMENTO	DETALLE DE ESTADO
1																					
2																					
3																					
4																					

Leyenda:
Tipo de Envío: Local
Tipo de Documento: Notificación, Resolución, Oficio, Constancia, Carta, otros
Estado de Documento: Entregado o Devuelto

Anexo Nº 06: Formato de Denuncia Policial

REPORTE DE PERDIDA DE DOCUMENTOS Y DENUNCIA POLICIAL

Nº	Tipo de documento extraviado o robado	Código o número del documento	Numero de guía	Correlativo del documento	Nombre del destinatario	Dirección del destinatario	Estado de documento

Leyenda:
Estado de Documento: Cargo o Correspondencia

Anexo Nº 07: Formato de Reporte Mensual

En vista vertical, pero deberá ser presentado en forma horizontal las 2 imágenes integradas en un mismo reporte de Excel.

FORMATO DEL REPORTE MENSUAL DE MENSAJERIA

OFICINA DE ONP

PERIODO :

ITEM	SEDE	MES	TIPO DE ENVIO	FECHA DE ORDEN (RECEPCION)	N° DE GUIA	CORRELATIVO DE GUIA	AREA USUARIA	TIPO DE DOCUMENTO	NUMERO DE DOCUMENTO	DESTINATARIO	DIRECCIÓN	DEPARTAMENTO	PROVINCIA	DISTRITO

Sede: Central
Tipo de Envio: Local
Tipo de Documento: Carta, Memo, Oficio,
Plazo de Entrega: Establecido en las Bases
Plazo de Devolución: Establecido en las Bases
Bajo Puerta: Solo llenar el campo con la palabra "SI", siempre y cuando el cargo haya sido entregado bajo puerta
Estado: Entregado, Devuelto, Pendiente, No Distribuido (Denuncia Policial)
Detalle de Estado: En los casos que sea una correspondencia devuelta, describir el motivo por la cual fue devuelta la correspondencia
Estado de Pago: Pagado o Pendiente

+

CORRESPONDENCIA								DENUNCIA POLICIAL POR PERDIDA O ROBO						
FECHA DE RECOJO DE LA CORRESPONDENCIA	PLAZO DE ENTREGA	FECHA 1ERA VISITA	FECHA DE ENTREGA AL DESTINATARIO	PLAZO DE DEVOLUCION	FECHA DE DEVOLUCION DEL DOCUMENTO CARGO (*)	GUIA DEVOLUCION	BAJA PUERTA?	FECHA DE PRODUCIDO EL HECHO	FECHA DE REGISTRO DE LA DENUNCIA	COMISARIA DONDE SE REGISTRO LA DENUNCIA	ESTADO	DETALLE ESTADO	PRECIO UNITARIO DEL SERVICIO	ESTADO DE PAGO

Anexo Nº 08: Estructura Mínima de Costos

	SERVICIO	DESTINO	CANTIDAD MENSUAL -2023 (REFERENCIAL)	CANTIDAD MENSUAL - 2024 (REFERENCIAL)	CANTIDAD MENSUAL -2025 (REFERENCIAL)
	Servicio Mensajería Express Lima Metropolitana Y Callao	LIMA METROPOLITANA Y CALLAO	8795	8199	8323
		TOTAL	8,795	8,199	8,323

NOTA: Los plazos para los destinos de este ítem se encuentran establecidos en el Anexo Nº 01.

	SERVICIO	DESTINO	CANTIDAD ANUAL-2023 (REFERENCIAL)	CANTIDAD ANUAL-2024 (REFERENCIAL)	CANTIDAD ANUAL-2025 (REFERENCIAL)	ESTIMADA (CANTIDAD TOTAL DEL SERVICIO)	PRECIO UNITARIO	PRECIO TOTAL
	Servicio Mensajería Express Lima Metropolitana Y Callao	LIMA METROPOLITANA Y CALLAO	105538	98386	99873	303797		
		TOTAL	105,538	98,386	99,873	303,797		

NOTA: Los plazos para los destinos de este ítem se encuentran establecidos en el Anexo Nº 01.

Anexo N° 9: Plan para la Vigilancia, prevención y control del COVID-19 en el trabajo, de acuerdo a la normativa vigente.

PLAN PARA LA VIGILANCIA, PREVENCIÓN Y CONTROL DE LA COVID-19 EN EL TRABAJO DE LA OFICINA DE NORMALIZACIÓN PREVISIONAL

DOCUMENTACIÓN PARA EL INGRESO DE PROVEEDORES A LAS INSTALACIONES EN EL CONTEXTO DE LA COVID-19:

1. Plan para la vigilancia, prevención y control de COVID-19 en el trabajo. La empresa de 1 a 4 trabajadores que no estén incluidos dentro del DS N°003-98-SA podrán registrar su plan a través del Formato simplificado (anexo 6) contenido en la Directiva Administrativa Nº 321-MINSA/DGIESP-2021 que establece las Disposiciones para la Vigilancia, prevención y control de la salud de los trabajadores con riesgo de exposición a SARS-CoV-2" y su modificatoria.
2. Registro de capacitación sobre los riesgos de exposición al SARS CoV- 2 y las medidas preventivas dentro del centro de trabajo.
3. Certificado de aptitud para el retorno a labores presenciales emitido por su médico ocupacional o quien haga sus veces conforme a lo dispuesto en la Directiva Administrativa Nº321-MINSA/DGIESP-2021 que establece las Disposiciones para la vigilancia, prevención y control de la salud de los trabajadores con riesgo de exposición A SARS-CoV-2" y su modificatoria.
4. Ficha de sintomatología COVID-19 según Directiva Administrativa Nº321-MINSA/DGIESP-2021, Anexo 02 y modificatoria (Con una antigüedad no mayor a 14 días).
5. Matriz IPERC de las actividades que realizarán dentro de las instalaciones, actualizada con las medidas preventivas frente al COVID-19.
6. Registros de equipos de protección personal (detallando los EPP), debidamente firmados por cada trabajador, de acuerdo con el riesgo expuesto. Considerar la entrega de equipos de prevención frente al COVID-19.
7. Constancia de SCTR, en caso la actividad este considerada en el Anexo N° 05 del D.S. N° 003-98 SA y modificatoria.
8. Certificado de Aptitud médica ocupacional vigente.
9. Carné o certificado digital de vacunación con esquema completa (De preferencia).

Anexo Nº 10 - Directiva DIR-02/01 Lineamientos de Seguridad de la Información.

Oficina de Normalización Previsional	Código: DIR-02/01 Inicio de vigencia: 15 MAR 2017

ONP

Oficina de Normalización Previsional

DIRECTIVA

LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

ROL	NOMBRE	CARGO	VISTO
Revisada por:	Juan Carlos López Bardales	Jefe de la Oficina de Tecnologías de la Información	
	Rodolfo Baca Gomez-Sanchez	Jefe de la Oficina de Gestión de Riesgos	
	Magin Viviano Bustinza	Jefe de la Oficina de Recursos Humanos	
	Enrique Mindreau Zelasco	Jefe de la Oficina de Administración	
	Hillman Farfán Ruiz	Jefe de la Oficina de Planeamiento, Presupuesto y Evaluación de Gestión	
	Miluska I. Gil Ramón	Jefa de la Oficina de Asesoría Jurídica	
Aprobada por:	Carlos Puga Pomareda	Gerente General	

1. OBJETIVO

Establecer lineamientos de Seguridad de la Información en la Oficina de Normalización Previsional, y dotar de instrumento normativo que oriente la adecuada administración de la información necesaria para el desarrollo de su gestión.

2. ALCANCE

La presente directiva es de cumplimiento obligatorio por todas las personas que prestan servicios bajo cualquier modalidad laboral o contractual y/o convenio en la Oficina de Normalización Previsional.

3. BASE LEGAL

3.1. Ley Nº 28496 que modifica la Ley N° 27815, Ley del Código de Ética de la Función Pública.
3.2. Ley N° 29733 – Ley de Protección de Datos Personales.
3.3. Ley Nº 30096, Ley de delitos informáticos.
3.4. Ley Nº 30171, Ley que modifica la Ley 30096.
3.5. Ley N° 30276 que modifica el Decreto Legislativo N° 822 - Ley sobre el Derecho de Autor, normas modificatorias y complementarias.
3.6. Decreto Supremo N° 043-2003-PCM, Aprueba Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
3.7. Decreto Supremo N°003-2013-JUS, Aprueban Reglamento de la Ley 29733, Ley de Protección de Datos Personales
3.8. Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnico Peruana "NTP – ISO/IEC 27001:2014 EDI 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.
3.9. Resolución Ministerial N° 174-2013-EF, que aprueba el Reglamento de Organización y Funciones de la Oficina de Normalización Previsional y su modificatoria.
3.10. Resolución Jefatural N° 070-2013-JEFATURA/ONP, aprueba el Manual de Organización y Funciones de la Oficina de Normalización Previsional y sus modificatorias.

4. RESPONSABILIDAD

La Oficina de Tecnologías de la Información y la Oficina de Administración son responsables de velar por el cumplimiento de lo dispuesto en la presente directiva, según sus competencias.

Todos los órganos y equipos de trabajo de la ONP son responsables de cumplir con lo dispuesto en la presente directiva.

5. DEFINICIONES

5.1. Activo de información

Es aquel elemento relevante en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución, en la que se distinguen tres niveles:

- La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.).
- Los Equipos/Sistemas/infraestructura/instalaciones que soportan esta información.
- Las Personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

5.2. Banco de datos personales

Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

5.3. Código móvil

Es un código de software que se transfiere desde una computadora a otra y luego se ejecuta automáticamente y realiza una función con poco o ninguna interacción con el usuario. El código móvil está asociado con un número de servicios middleware (es un software de conectividad que ofrece un conjunto de servicios que hacen posible el funcionamiento de aplicaciones distribuidas sobre plataformas heterogéneas).

5.4. Comité de Gestión de Seguridad de la Información

Se refiere a un cuerpo integrado por representantes de las áreas sustantivas de la Institución, designados mediante Resolución Jefatural, cuya responsabilidad es la de garantizar y promover la seguridad de la información en la ONP.

5.5. Controles criptográficos

Conjunto de técnicas que hacen posible el intercambio de mensajes por la red de manera segura, que garantiza que los mensajes sólo puedan ser leídos por los receptores a quienes van dirigidos.

5.6. Custodio de la Información

Es el responsable de resguardar los activos de información que utiliza y/o custodia, así como los medios en los cuales dichos activos residen o se soportan[1], aplicando controles de seguridad razonables con la finalidad de minimizar los riesgos respecto a la confidencialidad y/o disponibilidad y/o integridad de los mismos en el ámbito de sus funciones en el caso del personal de la ONP[2] y en el ámbito del marco contractual en el caso de los contratistas de servicios. Asimismo, el Custodio debe tener en consideración los controles dispuestos por el Propietario de la Información y debe coordinar su gestión con el Gestor de Seguridad de la Información, según

[1] Dependiendo del activo de información, podrá existir uno o más custodios de la información.

[2] Existen puestos en el Manual de Organización y Funciones que son custodios naturales (Logística, Oficina de Tecnologías de la Información, entre otras).

sea el caso. Todo el personal de la ONP es custodio de la información específica que recopila, trata y/o almacena para sus funciones.

5.7. **Datos personales**
Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados.

5.8. **Datos personales sensibles**
Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones lineamientos, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.

5.9. **Dispositivo móvil**
Son aparatos móviles de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente, conocidos como computadora de mano, "Palmtop", "Handheld", "Tablet", "Smartphones", etc.

5.10. **Evento**
Ocurrencia identificada que puede ser relevante para la seguridad de la información, la cual requiere seguimiento para evitar un potencial incidente.

5.11. **Hábeas Data**
Acción Constitucional a la que se puede acudir para: 1) Acceder a información que obre en poder de cualquier entidad pública, ya se trate de la que generen, produzcan, procesen o posean, incluida la que obra en expedientes terminados o en trámite, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier otro documento que la administración pública tenga en su poder, cualquiera que sea la forma de expresión, ya sea gráfica, sonora, visual, electromagnética o que obre en cualquier otro tipo de soporte material; y 2) Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales.

5.12. **Incidente de seguridad de la información**
Evento o serie de eventos indeseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y que atenta contra la seguridad de la información y sus características de confiabilidad, disponibilidad e integridad.

5.13. **Propietario de la información**
Es el responsable de clasificar el nivel de confidencialidad de la información y de definir qué usuarios (custodios de la información) deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencias. Asimismo, es el responsable de coordinar con el Gestor de

Seguridad de la Información las medidas de seguridad aplicables para proteger los activos de información.

5.14. **Sistema de información**
Conjunto organizado de elementos que interactúan entre sí para tratar los datos y la información (incluyendo procesos manuales y automáticos). Estos elementos son de 4 tipos: Personas, Datos, Actividades o técnicas de trabajo y Recursos materiales en general (típicamente recursos informáticos y de comunicación, aunque no tienen por qué ser de este tipo obligatoriamente).

5.15. **Titular de datos personales**
Persona natural a quien corresponden los datos personales. Si la persona natural es externa a la institución se refieren a ciudadanos, si es interna se referirá a personal de la ONP y sus proveedores.

5.16. **Titular del banco de datos personales**
Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad, que debe ser designada por la Jefatura de la Entidad.

5.17. **Tratamiento de datos personales**
Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos.

6. ABREVIATURAS

ONP	:	Oficina de Normalización Previsional
BD	:	Base de Datos
CGSI	:	Comité de Gestión de Seguridad de la Información
COSI	:	Comité Operativo de Seguridad de la Información
MOF	:	Manual de Organización y Funciones
OAD	:	Oficina de Administración
OAJ	:	Oficina de Asesoría Jurídica
OPG	:	Oficina de Planeamiento, Presupuesto y Evaluación de la Gestión
ORH	:	Oficina de Recursos Humanos
OTI	:	Oficina de Tecnologías de la Información
TI	:	Tecnologías de la Información

7. DISPOSICIONES GENERALES

7.1. A fin de garantizar la aplicación de las medidas de seguridad de la información establecidas por la ONP, así como optimizar su gestión, la entidad se soportará en el CGSI, COSI, el Gestor de Seguridad de la Información, los propietarios de la información, los custodios de la

información y el personal asignado para cumplir roles de seguridad en los diferentes órganos[3].

7.2. Para la ejecución y despliegue de los lineamientos de seguridad de la información, la ONP se apoyará en los diferentes órganos de la institución.

a. La OTI es la encargada de administrar, controlar y actualizar el presente documento. Asimismo, establecerá las normas y procedimientos que regulen cada lineamiento referido a la protección de la información de la ONP.
b. El Gestor de Seguridad de Información, en coordinación con los responsables de los órganos, establecerán medidas de seguridad para regular nuevas necesidades de acceso físico o lógico por parte de terceros a los activos de información de la ONP.
c. La Oficina de Recursos Humanos y el Equipo de Trabajo de Logística deberá verificar que en todos los contratos, ya sea de prestación de servicios personales, consultorías, servicios, implementación de soluciones, etc., se incluyan términos relacionados a la seguridad de la información, relacionados con los siguientes aspectos:
   i. Requerimientos de seguridad.
   ii. Controles de seguridad a aplicar por el tercero.
   iii. Compromisos de confidencialidad aplicables al caso.
   iv. Condiciones de gestión de los servicios.

d. Los contratos de servicios para la administración y control de los sistemas de información, redes y/o ambientes de procesamiento de información de la ONP, contemplarán los siguientes requerimientos de seguridad cómo mínimo:
   i. Cumplimiento de los presentes Lineamientos de Seguridad de la Información de la ONP, por parte de la empresa contratista.
   ii. Forma en que cumplirán la normativa legal aplicable.
   iii. Controles de seguridad requeridos para proteger los activos de información.
   iv. Responsabilidades de instalar y dar mantenimiento de hardware y software.
   v. Establecimiento de un proceso de gestión de cambios.
   vi. Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información de la ONP.
   vii. Declaratoria de compromiso de informar los incidentes de seguridad de Información a la ONP, determinar acciones para su investigación y brindar facilidades al personal de la ONP para realizar las investigaciones.
   viii. Acuerdos de niveles de servicios.
   ix. Establecimiento de un proceso de escalamiento para resolución de problemas.
   x. Mantenimiento de documentación actualizada de los sistemas.
   xi. Medios para garantizar que todas las partes involucradas en la prestación de un servicio incluyendo subcontratistas, conozcan sus responsabilidades en materia de seguridad de la información.

[3] Los Comités referidos tiene definidas sus funciones de acuerdo a Resolución Jefatural del titular del Pliego (Nro. 027-2015-Jefatura/ONP) y las funciones del gestor de Seguridad de la Información están definidas en el MOF.

xii. Forma en la que se mantendrá y comprobará la protección de la integridad, disponibilidad y confidencialidad de los activos de información.
xiii. Requerimientos de continuidad de los servicios y de la información ante la ocurrencia de un desastre o interrupción inesperada.
xiv. Consideraciones de propiedad intelectual, propiedad de software y derechos reservados en caso se requiera.
xv. Derecho de auditoría por parte de la ONP sobre los contratistas de servicios contratados.

7.3. Los Lineamientos de Seguridad de la Información brindan directrices para garantizar la confidencialidad, integridad y disponibilidad de la información, y a su vez mejorar la calidad y disponibilidad de los servicios que la ONP ofrece a sus clientes internos y externos.

7.4. En la ONP se reconoce como activos estratégicos de la Institución a los datos, la información y los sistemas que la soportan, por lo que manifiestan su compromiso de alcanzar los niveles de seguridad necesarios que aseguren su protección.

7.5. En la ONP se respalda activamente la seguridad dentro de la organización a través de una dirección clara, un compromiso apropiado, recursos adecuados y conocimiento de las responsabilidades en la seguridad de información.

7.6. Esta directiva abarca a todos los activos de información usados en la ONP para el desarrollo de sus actividades y por ende es aplicable obligatoriamente para todos los involucrados en el uso de los mismos, así como de los sistemas que los soportan.

7.7. Todo activo de información de la ONP, cualquiera sea la forma que adopte, debe ser protegido de los riesgos de pérdida de confidencialidad, integridad y disponibilidad.

7.8. La información y las tecnologías de información deberán ser usadas para los propósitos de la ONP, debiendo aplicarse el uso adecuado de los bienes del estado señalado en el Código de Ética de la Función Pública, Ley N°27815, cuando no exista un lineamiento o normativa explicita para su utilización.

7.9. Todo recurso tecnológico, sistema informático y, en general cualquier actividad realizada en el entorno del trabajo de los sistemas de información deberá proveer un mecanismo o procedimiento confiable de identificación de manera individual e inequívoca del usuario.

7.10. El personal debe alertar, de manera oportuna y brindando el mayor detalle, cualquier incidente que atente contra lo establecido en los Lineamientos de Seguridad. El responsable inmediato superior deberá analizar cada caso y consultarlo o reportarlo al Gestor de Seguridad de la Información de la ONP de manera que se adopten las medidas correspondientes para evitar su repetición.

7.11. La ORH y la OAD exigirán a todos los involucrados en el manejo de información institucional, la firma de un Acuerdo de Confidencialidad, para

evitar manejos indebidos de dicha información. (Formato DIR-02/01-A: Acuerdo de Confidencialidad)

7.12. La ONP se reserva el derecho de revocar el privilegio de acceso a la información y a las tecnologías que la soportan al personal que considere pertinente.

7.13. La ONP se reserva el derecho de tomar medidas administrativas y acciones legales, conforme a lo que establece el Reglamento Interno para los Servidores de la ONP, así como en las normas de contrataciones del Estado, según corresponda.

7.14. Toda utilización, ingreso, copia o interferencia indebida con fines de alterar, dañar o destruir los activos de información existentes en la ONP, podrá ser considerada y catalogada como "Delito contra Datos y Sistemas Informáticos", según el Capítulo II de la Ley N° 30096. Si los actos antes indicados se han ejecutado haciendo uso de información reservada o si el agente pone en peligro la defensa, seguridad y soberanía nacionales, estas acciones podrían ser catalogadas como "Agravantes", según el Capítulo VII, artículo 11, numerales 2 y 4 de la Ley N° 30096.

7.15. Se prohíbe que en los equipos de cómputo se mantenga, promueva, fabrique, distribuya, exhiba, ofrezca, comercialice, publique, importe o exporte, objetos, libros, escritos, imágenes visuales o auditivas de carácter pornográfico. La inobservancia a esta prohibición será considerada como incumplimiento a los lineamientos de seguridad de la información, señalados en los Lineamientos de Cumplimiento del numeral 8.12.

7.16. Cuando el material pornográfico esté referido a menores de edad, además de la falta administrativa antes mencionada; se configura el Delito de Pornografía Infantil según el artículo N° 183-A del Código Penal, modificado por la Cuarta Disposición Complementaria Modificatoria de la Ley de Delitos Informáticos. La instancia que tome conocimiento de tales hechos, deberá reportarlos a la OAJ de la ONP para que se presente la denuncia correspondiente ante el Ministerio Público en caso corresponda.

7.17. Toda acción realizada con los recursos de información e informática proporcionada por la ONP que vulnere las normativas administrativa o legal será sancionada según corresponda conforme al Código de Ética de la Función Pública y la Ley del Servicio Civil.

7.18. El Equipo de Trabajo de Logística de la OAD deberá verificar que en los términos de referencia de los servicios, se incluyan como requisito, la designación de un responsable, quién coordinara los temas de seguridad de información con el Gestor de Seguridad de la Información de la ONP.

7.19. En los casos que existan nuevos recursos de procesamiento de la información, los órganos o equipo de trabajo responsables deberán comunicar y coordinar con la OTI la implementación de los controles de seguridad necesarios.

7.20. El uso de equipos o dispositivos personales que puedan representar amenazas contra los activos de información serán evaluados y aprobados por la OTI.

7.21. Los Lineamientos de Seguridad de la Información se han clasificado por su naturaleza en los siguientes lineamientos:

Lineamiento	Descripción
Lineamientos de seguridad de los Recursos Humanos	Lineamientos para asegurar que el personal tenga presente sus roles y responsabilidades, y considere los riesgos de seguridad de la información, así como para definir el marco apropiado para el entrenamiento del personal en los aspectos de seguridad relacionados con su actividad.
Lineamientos de administración de activos.	Lineamientos para garantizar que los activos de información reciban un apropiado nivel de protección y uso, en función al grado de sensibilidad que presenten.
Lineamientos de Control de accesos	Lineamientos para controlar que el acceso a los datos, sistemas de información, instalaciones de procesamiento y procesos de la ONP, sean otorgados en función de las tareas y responsabilidades de cada usuario y para definir las reglas de autorización y responsabilidades en la creación de nuevos accesos.
Lineamientos de Controles Criptográficos	Lineamientos para asegurar el uso adecuado y eficaz de la criptografía, para asegurar la confidencialidad e integridad de la información.
Lineamientos de seguridad física y ambiental	Lineamientos para prevenir accesos no autorizados a los ambientes físicos de la ONP, donde se almacena y/o procesa información sensible y para evitar daño, modificación, pérdida o mal uso de la información o de los activos de información que la soportan.
Lineamientos de seguridad de las operaciones	Lineamientos para asegurar el funcionamiento correcto y seguro de las facilidades de información y para definir una gestión que permita un balance adecuado entre seguridad y funcionalidad de los servicios de procesamiento para el desarrollo de las actividades de la ONP.
Lineamientos de seguridad de las comunicaciones	Lineamientos para asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.
Lineamientos de adquisición, desarrollo y mantenimiento de sistemas	Lineamientos para asegurar que todos los sistemas de información actuales y nuevos incluyan requerimientos de seguridad para proteger la confidencialidad, integridad y disponibilidad de los datos que manejan.
Lineamientos de Relaciones con proveedores	Lineamientos para asegurar la protección de los activos de la organización a que tienen acceso los proveedores.
Lineamientos de gestión de los incidentes de seguridad de la información	Lineamientos para asegurar que el personal afectado comunique oportunamente a los responsables de seguridad, los eventos o debilidades asociados con la seguridad de información.

Lineamiento	Descripción
Lineamientos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	Lineamientos para responder ante interrupciones de las actividades de la ONP y proteger los procesos críticos ante los efectos de una falla mayor por problemas relacionados a la seguridad de la información, así como para minimizar el impacto en la organización y recuperarse de una pérdida de los activos de información principales por un desastre.
Lineamientos de cumplimiento	Lineamientos para asegurar el cumplimiento de los lineamientos y normativas de seguridad de la información de la ONP.

8. DISPOSICIONES ESPECÍFICAS

8.1. LINEAMIENTOS DE SEGURIDAD PARA EL RECURSO HUMANO

8.1.1. Objetivos

a. Asegurar que el personal, tenga presente sus roles y responsabilidades y considere en forma permanente los riesgos de seguridad de la información.
b. Definir el marco apropiado para el entrenamiento del personal en los aspectos de seguridad relacionados con su actividad laboral, de acuerdo a los objetivos y requerimientos de seguridad de la ONP.

8.1.2. Alcance

Este lineamiento se aplica a todas las personas que presten servicios bajo cualquier modalidad laboral o contractual y/o convenios en la ONP que tengan acceso a los activos de información de la ONP.

8.1.3. Previo al empleo: Selección del personal

a. Se verificarán los antecedentes de los candidatos de acuerdo a la legislación aplicable y los principios éticos de la ONP.
b. Los roles y responsabilidades en seguridad de información estarán definidos en el Reglamento Interno de Trabajo para el personal de la ONP, en los convenios y en los términos de contratación para el personal de terceros. Las responsabilidades del personal, deben incluir la protección de los recursos de información de la entidad respecto a los accesos, divulgación, modificación o destrucción no autorizada.
c. Todo formulario, entrevista o contrato con el postulante advertirá explícitamente que su documentación podrá ser verificada y que si existiera discrepancias, estas podrán ser investigadas.
d. Todo contrato que establezca un vínculo laboral y/o contractual con la ONP deberá incluir cláusulas de compromiso a título personal que preserven la confidencialidad de la información de la ONP. A su vez, se deberá evidenciar la recepción y firma de un compromiso de cumplimiento de los Lineamientos de Seguridad de la información de la ONP. (Formato DIR-02/01–B Compromiso de Cumplimiento de Lineamientos de Seguridad de la Información de la ONP).

8.1.4. Durante la permanencia del personal

a. No se deberá vulnerar o intentar vulnerar los sistemas de cómputo y redes internas o externas, de personas particulares u otras organizaciones, haciendo uso de los recursos otorgados por la ONP ya sea dentro o fuera del horario laboral. En caso se detecten infracciones a la seguridad de información, la ONP deberá seguir el proceso disciplinario formal para iniciar sanción administrativa o acción legal según corresponda de acuerdo a los lineamientos vigentes que considere la ORH o la OAD de acuerdo a la normativa vigente.
b. El personal que cumple funciones para la ONP deberá ser capacitado periódicamente en los aspectos referentes a los lineamientos y normativas de seguridad, así como sus responsabilidades respecto a la protección de la información. Se podrá utilizar diversos medios educativos para dicha labor.

8.1.5. Desvinculación o cambio de responsabilidades de empleo

a. Para el caso de la desvinculación laboral, el personal deberá entregar mediante un cargo, todos los bienes o materiales con información de la ONP al responsable del órgano o del equipo de trabajo responsable de su supervisión, de acuerdo a los lineamientos señalados en la directiva Gestión Administrativa y de Recursos Humanos vigente.
b. Todos los accesos a la información, permisos y privilegios de los sistemas de información, accesos a las áreas de la institución y recursos de la red de datos, deberán ser removidos inmediatamente después de que el personal concluya su contrato. Para ello, el responsable asignado en el órgano o equipo de trabajo, deberá solicitar a la OTI la cancelación de los accesos informáticos del personal al término de su vínculo contractual.
c. El acceso a las instalaciones de la ONP a nivel nacional, deberá quedar restringido para el personal, ni bien quede extinguido su vínculo contractual.

8.2. LINEAMIENTOS DE ADMINISTRACION DE ACTIVOS

8.2.1. Objetivo

Garantizar que los activos de información reciban un apropiado nivel de protección y uso, en función al grado de sensibilidad que presenten.

8.2.2. Alcance

Este grupo de lineamientos aplica a todo dato e información que sea de propiedad de la ONP o que se encuentre bajo su custodia, con el fin de definir los niveles de protección y medidas de tratamiento de acuerdo a su clasificación.

8.2.3. Normas generales

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a

la funcionalidad que cumplen, debiendo ser rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

8.2.4. Responsabilidad por los activos

a. Entendiéndose el concepto de Activos de Información, de acuerdo a lo señalado en el numeral 5.1 de la presente directiva, se deberá de elaborar y mantener un inventario de los Activos de información. Dichos inventarios podrán ser consolidados y almacenados de manera física y/o lógica.
b. Todos los activos de información deberán tener asignado un propietario el cual será responsable del mantenimiento de los controles adecuados. La implantación de controles específicos podrá ser delegada por el propietario según lo estime conveniente, no obstante, el propietario permanecerá como responsable de la adecuada protección de los activos.
c. El Gestor de Seguridad de la Información conjuntamente con el Propietario de la Información, deberán realizar la clasificación de la misma, considerando lo establecido en la Ley de Transparencia y Acceso a la Información Pública, con el objeto de establecer su uso aceptable, modalidad de tratamiento y protección. A su vez, los activos asociados a la información, clasificada por la ONP como **reservada o confidencial**, deberán mantenerse en un inventario detallando el propietario de los mismos, de acuerdo a la clasificación descrita en el numeral 8.2.5. Para ello, cada órgano o equipo de trabajo designará a un encargado de la documentación y actualización del inventario de la información. El Gestor de Seguridad de la Información consolidará todos los inventarios verificando su clasificación.
d. El personal deberá devolver todos los activos que estén en su poder como consecuencia de la finalización de su relación laboral, contractual o convenio con la ONP.

8.2.5. Clasificación de la información

a. La clasificación de la información debe estar documentada de manera detallada y formal en el marco de los Lineamientos de Seguridad de la Información, indicando los pasos, actividades, responsables y alcances principales para su clasificación, conservación, custodia, protección, deshecho, entre otros.

b. Para efectos de la presente directiva la información generada por la institución y bajo su custodia, será también clasificada considerando lo establecido en la Ley de Transparencia y Acceso a la Información Pública, en:

   i. **Información Pública**.
   ii. **Información Reservada.**
   iii. **Información Confidencial**.

c. La clasificación de la información se realizará por lo menos una vez al año, no obstante cuando se estime que una información ha cambiado, su nivel de clasificación deberá modificar su tipología en forma inmediata y reportarse al Gestor de Seguridad de la Información.

8.2.6. Manejo de la información

a. La ONP es propietaria única y exclusiva de toda la información de la organización, la cual dependiendo de su clasificación, debe ser identificada, controlada y protegida. Por tal motivo todo acceso a la información electrónica de la ONP debe ser autorizado, identificado y controlado por el propietario de la información.
b. Se deberán contemplar las medidas para asegurar la confidencialidad, integridad y disponibilidad de la información de la ONP, tomando en consideración que ésta puede estar contenida en sistemas informáticos, en medios portátiles y extraíbles, transmitida a través de redes o entre sistemas, impresa o escrita.
c. La impresión o copias de información clasificada como **Confidencial** deberá estar autorizada expresamente mediante correo o documento administrativo por el responsable que la ha clasificado como tal, el cual debe haber sido designado por el propietario de la información. De existir impresiones o copias adicionales éstas deberán ser eliminadas haciendo uso de los procedimientos establecidos para dicho fin.
d. Todos los envíos de Información clasificada como **reservada o confidencial**, deben ser realizados por medios de transporte de información que brinden seguridad en su traslado. En tal sentido, el uso de cuentas de correo personales, no institucionales, para estos fines está terminantemente prohibido. Así mismo, desde la red ONP sólo estará habilitado el uso del correo institucional y no de correos externos. Se podrán hacer excepciones sustentadas en necesidades específicamente laborales.
e. Toda divulgación de información electrónica clasificada como reservada o confidencial, al exterior de la ONP, deberá contar con la aprobación formal correspondiente del responsable que la clasificó como tal, el cual debe haber sido designado por el propietario de la información.
f. Solo se podrá acceder, procesar o almacenar, en los equipos asignados o en servidores de la red de datos y en el entorno físico de trabajo, información lógica o física que esté de acuerdo a sus funciones.
g. Todo recurso tecnológico de información reservada o confidencial, deberá contar con medidas de seguridad física, a fin de evitar riesgos que pongan en peligro el recurso en sí o la información que contiene.
h. Las normas, controles o procedimientos pertinentes para evitar los riesgos contra manipulaciones indebidas de los activos de información (equipos informáticos, de comunicación, medios de almacenamiento, documentos, etc.), cambio de sus partes, robos parciales o totales, deberán ser coordinados con el Gestor de Seguridad del Equipo de Trabajo de Logística de la OAD y el Gestor de Seguridad de Información a través del órgano o equipo de trabajo de la supervisión de los servicios.

8.3. LINEAMIENTOS DE CONTROL DE ACCESO

8.3.1. Objetivos

a. Controlar que el acceso a los datos, sistemas de información, instalaciones de procesamiento y procesos de la ONP, sea otorgado en función de las tareas y responsabilidades de cada usuario.
b. Definir las reglas de autorización y responsabilidades en la creación de nuevos accesos.

8.3.2. Alcance

Este grupo de lineamientos aplican a toda la información de la ONP o bajo su custodia, los sistemas que la soportan y todos los medios en la que se almacena y que se encuentran bajo la administración de la ONP y de sus servicios.

8.3.3. Norma general

Con el fin de lograr una efectiva protección de los recursos de información de la ONP, es indispensable tener la capacidad de otorgar los accesos de acuerdo a las necesidades reales de los usuarios, considerando el principio del "menor privilegio posible", es decir, se debe asignar a cada usuario únicamente el nivel de acceso necesario para cumplir con sus funciones.

8.3.4. Requerimientos para el control de acceso

a. Al definir los niveles de accesos de los sistemas o servicios deben basarse en los requisitos del negocio y de seguridad de información.
b. Todos los proyectos que involucren tecnologías de información, deben considerar los requerimientos de seguridad para el control de accesos.

8.3.5. Gestión de acceso de los usuarios

a. Se deben mantener actualizados los procedimientos para la solicitud, atención, asignación, modificación y baja de accesos a la plataforma tecnológica de la ONP y a sus sistemas de información de acuerdo a las necesidades de seguridad y de negocio de la ONP. Dichos procedimientos deberán incluir niveles adecuados de autorización.
b. Se implementará, en la medida de las posibilidades técnicas, un mecanismo que permita la integración de la asignación o remoción de derechos de accesos de los usuarios, a todos los sistemas y servicios de red.
c. Las cuentas de acceso a los sistemas deben ser inactivadas cuando el titular de la cuenta culmine el vínculo laboral, contractual o convenio, asimismo deberán bloquearse las cuentas de correo electrónico temporalmente cuando el usuario se encuentra de licencia, salvo excepciones solicitadas por los directores o jefes de órganos, por lo que, en el caso de la cuenta de correo electrónico, se recomienda colocar un aviso de ausencia temporal. Todo cambio, incluyendo los cambios de rotación del personal, deberán ser reportados oportunamente a la ORH o Supervisiones de los Servicios por las áreas de la ONP.
d. La OTI evaluará y aprobará el uso de las cuentas con acceso total a las aplicaciones y sistemas informáticos por parte de usuarios específicos, que por sus labores dentro de la ONP requieran de dichos accesos.
e. En la medida de las posibilidades técnicas, los sistemas de la ONP solicitarán automáticamente el cambio de contraseña de acceso al primer inicio de sesión en el correspondiente sistema y debiendo solicitar periódicamente el cambio de la misma.
f. El personal a quien se le entregue una cuenta y/o contraseña con accesos privilegiados ("administrador") de sistemas, aplicaciones, software, equipos de comunicación, entre otros, deberá firmar un

documento de "Declaración de Responsabilidad de Uso de Cuentas Privilegiadas". Este tipo de cuentas es de asignación excepción y deberá ser justificado operativamente.

g. Para mantener la responsabilidad sobre el acceso a los sistemas y red de la ONP, se asigna cuentas individuales. El uso de cuentas grupales (una cuenta para varias personas) sólo será permitido cuando sea necesario por razones de operación, siendo requerido para ello una autorización por parte del jefe del órgano correspondiente. Adicionalmente se requerirá la verificación y aprobación de la OTI.

8.3.6. Responsabilidad del personal

a. El personal que tenga acceso a la información o a los sistemas de información es responsable de:
   i. El uso adecuado de sus contraseñas de acceso.
   ii. No compartir sus contraseñas de acceso.
   iii. No acceder a la información física o lógica a la cual no tiene permisos correspondientes.
   iv. Adoptar los mecanismos más adecuados con la finalidad de preservar la información, en los casos que se ausente de su puesto de trabajo.

b. El correo electrónico es una herramienta de trabajo, que sobre la base de una adecuada utilización permite al personal tener un acceso una rápida y eficiente comunicación, para propósitos relacionados con las funciones de la organización. Los correos electrónicos son considerados documentos oficiales propiedad de la ONP para todo uso. Por tal motivo se prohíbe al personal utilizar correos electrónicos que no le han sido asignados, usar lenguaje obsceno y/o abusivo en el contenido de los mismos, emplearlos para uso personal o para fines que se encuentren fuera de las funciones asignadas

c. Está prohibido que un usuario acceda en forma local o remota a un computador que no le ha sido asignado, a menos que cuente con la debida autorización expresamente mediante correo, por el propietario de dicho equipo o por el jefe inmediato de dicha persona.

8.3.7. Control de acceso a la red de la ONP

a. Todos los usuarios deberán tener el acceso a los servicios y sistemas específicos de acuerdo a sus necesidades reales y para los cuales ellos han sido autorizados.

b. Para el caso de acceso remoto a la red de sistemas de la ONP, se debe definir por lo menos un sistema de autenticación del usuario.

c. En el caso de acceso remoto entre oficinas (redes WAN), se deben conectar a través de una red privada. Para los casos en que la conexión sea a través de una red pública compartida como Internet, se utilizarán mecanismos de encriptación y autenticación de la conexión.

d. Todos los puertos de diagnóstico lógicos y físicos de los equipos de red, seguridad o gestión, estarán deshabilitados, salvo alguna necesidad puntual de funcionalidad autorizada por el Equipo de Administración de Plataformas y Redes de la OTI en coordinación con el Gestor de Seguridad de la Información.

e. El diseño topológico de la red debe seguir las recomendaciones de segmentación, según áreas, pisos, y especialmente para los sistemas o servicios críticos. Los esquemas de segmentación propician la instalación de mecanismos de control de acceso y protección contra ataques a los servicios tecnológicos, provenientes de personal o sistemas que se encuentren al interior de la ONP.
f. Todos los puntos de conexión a la red deben ser controlados para no permitir conexiones no autorizadas. Los puntos de red que no sean utilizados en el corto plazo o que no se usan, deben permanecer deshabilitados. Este cuidado debe tenerse en cuenta en redes compartidas con otras organizaciones o servicios.
g. La configuración de la red de la ONP deberá considerar controles de enrutamiento que deberán ser implementados con el fin de asegurar que sólo se permitan conexiones y accesos a información autorizados.
h. La responsabilidad sobre el uso de los computadores portátiles, y por lo tanto de la información contenida en ellos, es del usuario que tiene asignado dicho bien. Se prohíbe el uso compartido con personas ajenas a los procesos de la institución

8.3.8. Control de acceso al sistema operativo

a. Los pasos básicos para acceder a la red de la ONP consideran los siguientes puntos:
   i. Límite del número de intentos de acceso no válidos a tres (podrá ser evaluado una vez al año por la OTI).
   ii. Cuando las capacidades técnicas de los sistemas de gestión de accesos lo permitan, las contraseñas o claves de acceso deberán ser configuradas mediante un esquema seguro con complejidad de caracteres y almacenadas en los sistemas haciendo uso de un algoritmo de encriptación seguro. Asimismo, las claves de acceso deberán ser transmitidas por la red de manera encriptada.
   iii. Los sistemas no deben permitir que las claves de acceso sean visualizadas al momento de ser ingresadas.
   iv. Las claves deben ser modificadas periódicamente.

b. Todos los usuarios deben tener un único código de identificación en la red para su uso personal. Esto incluye a los administradores de red, administradores de base de datos, soporte técnico, operadores y programadores.
c. El método para autenticar a los usuarios en la red es la clave (password o contraseña), sin embargo, cuando sea necesario un nivel de autenticación superior en sistemas críticos puntuales se podrán utilizar otros métodos tales como: tokens, smart cards o dispositivos biométricos.
d. El uso de cualquier software utilitario en la red de la ONP, deberá ser evaluado por el personal de la OTI. Asimismo, la autorización de uso deberá ser restringida a tareas específicas y controladas.
e. Las sesiones deberán bloquearse automáticamente después de un tiempo determinado de inactividad.

8.3.9. Control de acceso a las aplicaciones e información

a. Todos los accesos creados en las aplicaciones de la ONP, deberán estar asociados a perfiles previamente definidos y aprobados.
b. Los sistemas informáticos que contienen información sensible para la organización deberán utilizar equipamiento informático dedicado o compartido con otras aplicaciones siempre y cuando estos no afecten el procesamiento y performance de los primeros.
c. Los usuarios deberán tener un único código de identificación por sistema de información del que sean usuarios. En la medida de las posibilidades técnicas se impulsará el uso de un único código, tanto para el acceso a la red como a los sistemas de información.
d. Las contraseñas de acceso a los sistemas informáticos deberán ser robustas, deben contener como mínimo 8 caracteres que contengan combinaciones de símbolos, caracteres alfanuméricos, mayúsculas y minúsculas.

8.4. LINEAMIENTOS DE CONTROLES CRIPTOGRÁFICOS

8.4.1. Objetivos

a. El objetivo del presente dominio es establecer los lineamientos relacionados al uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

8.4.2. Alcance

a. Este lineamiento aplica a todos los accesos a la información que se requieran habilitar por parte de la ONP a proveedores de servicio y/o entidades con las que se desee compartir información.
b. Este lineamiento abarcará a cualquier medio de acceso a la información de la ONP, sean aplicativos, BD, redes corporativas, Wireless y redes externas

8.4.3. Uso de Controles Criptográficos

a. Se debe formular e implantar procedimientos para el uso de Controles Criptográficos donde se considere el medio y la forma de cómo se procesan, transfieren y comparten información entre usuarios de la ONP, proveedores de servicio y otras entidades colaboradoras.
b. La OTI deberá analizar y evaluar la inclusión de un estándar de uso de Controles Criptográficos en las aplicaciones para la entidad. Este estándar debe contener el detalle respecto al algoritmo, tamaño, gestión de las llaves, el soporte de las técnicas de encriptación y el alcance del mismo según el tipo de aplicación
c. La OTI definirá la gestión de las llaves de encriptación incluyendo la protección contra modificación, pérdida y destrucción. Las llaves secretas o privadas o llaves maestras que se generen deberán estar bajo la custodia de la OTI.
d. La OTI establecerá los protocolos para el envío de información considerada interna o confidencial a partes terceras, que incluirán como

mínimo la definición de la forma de la solicitud, los mecanismos de seguridad del envío, las autorizaciones requeridas y la responsabilidad sobre el tratamiento de la misma, en coordinación con él Gestor de Seguridad de la Información. Estas solicitudes deberán ser recibidas mediante Carta, Oficio o Memorándum dirigidas al Jefe del órgano de la ONP responsable y al Jefe de la OTI.

e. Los controles criptográficos deben ser utilizados para alcanzar diferentes objetivos de seguridad como por ejemplo:
   i. **Confidencialidad:** utilizando cifrado de información para proteger información sensible o crítica, así sea transmitida o almacenada.
   ii. **Integridad/Autenticidad**: utilizando firmas digitales o códigos de autentificación de mensajes para proteger la autenticidad e integridad de la información crítica o sensible que es almacenada o transmitida.
   iii. **No repudio:** utilizando técnicas criptográficas para obtener prueba de ocurrencia o no ocurrencia de un evento o acción.

8.4.4. Gestión de Claves

a. Se deberán proteger todos los tipos de claves de su modificación o destrucción; las claves secretas y las privadas además requieren protección contra su distribución no autorizada. Con este fin también pueden usarse técnicas criptográficas.
b. El sistema de gestión de claves se deberá basar en un conjunto acordado de normas, procedimientos y métodos seguros para generar, asignar, distribuir, cambiar, revocar, actualizar, dar seguimiento, generar respaldo y destrucción de las mismas.

8.5. LINEAMIENTOS DE SEGURIDAD FÍSICA Y AMBIENTAL

8.5.1. Objetivos

a. Prevenir accesos no autorizados a los ambientes físicos, en los cuales se almacena y/o procesa información institucional.
b. Evitar el daño, modificación, pérdida o mal uso de la información o de los activos de información que la soportan, haciendo uso de las vías de accesos físicas.

8.5.2. Alcance

a. Este lineamiento aplica a todos los activos de información de la ONP, sean éstos computadoras, componentes de red o información digital o impresa, de propiedad de la ONP, administrados por ella o generado como parte de los servicios que se brinden a la ONP.
b. En atención a que los activos de información se mantienen físicamente en dependencias u oficinas de la ONP. El presente lineamiento se orienta a la protección de estos espacios, además de los activos de información.

8.5.3. Áreas Seguras

a. La información calificada como **Confidencial**, así como los sistemas de procesamiento de información principales, deben ser protegidos en "áreas seguras" entendiendo por ello lugares donde se proporcione un nivel de seguridad razonable para protegerlos contra accesos físicos no autorizados, modificación, robo o daño de la información en base a defensas perimetrales y controles de acceso.
b. Todas las "áreas seguras" deberán tener al menos un mecanismo de detección de intrusiones o alarma electrónica que funcione aún fuera de horario de oficina.
c. El Gestor de Seguridad de la OAD en coordinación con los responsables de los órganos, deberán definir e identificar en un plano, los ambientes de acceso restringido, considerando la implementación de un procedimiento de registro de visitantes.
d. Todas las "áreas seguras" que tengan "zonas de acceso restringido" deberán contar con un personal de seguridad asignado que autorice los accesos físicos. Asimismo, debe elaborarse una lista de personas autorizadas a ingresar.
e. El personal de seguridad asignado deberá llevar el registro y a su vez conocer todos los ambientes identificados como "zona de acceso restringido" con el objetivo de gestionar su protección.
f. Los Centros de Cómputo no deben ser usados para otro fin que no sea el procesamiento de información. El acceso a dichos ambientes debe estar controlado mediante algún mecanismo seguro, como puertas con llaves, dispositivos de control de acceso por aproximación, biometría u otros que asegure el acceso sólo al personal autorizado.

8.5.4. Controles de ingreso

a. La OAD de la ONP deberá mantener actualizados los procedimientos y controles de ingreso del personal o visitantes a las instalaciones en que ONP realice sus operaciones.
b. Estos controles deben incluir como mínimo el registro de ingreso y salida, con hora y fecha, ya sea por parte del personal de seguridad del local o a través de los sistemas automáticos de control de ingreso.
c. El ingreso de visitas debe ser previamente autorizado ante el personal de seguridad del local, haciendo entrega de su documento de identidad, el cual deberá quedar en custodia de ONP mientras dure su visita. En este caso debe registrarse como mínimo:
   i. Hora de ingreso.
   ii. Persona visitada y área a la cual pertenece.
   iii. DNI, carné de identidad, pasaporte, y firma del visitante.
   iv. Motivo de la visita.
   v. Hora de salida.
   vi. Autorización de la persona que indicó el ingreso.
   vii. Si ingresó con algún equipo o dispositivo, se debe detallar las características únicas que lo identifiquen.
d. Dentro de las instalaciones de la ONP, el personal, proveedores y visitantes deberán usar su fotocheck en un lugar visible.

e. Está prohibido el uso de cámaras de video o fotografía en las oficinas de la ONP, salvo, casos debidamente justificados y aprobados por la Oficina de Administración y/o la OTI.
f. En el Centro de Cómputo y en todas las instalaciones en donde se encuentren dispositivos de distribución y de procesamiento de datos está prohibido que las visitas ingresen con teléfono celular o dispositivos tablets, computadores portátiles o cualquier dispositivo, medio extraíble de transporte y almacenamiento de datos, salvo los casos técnicamente justificados y aprobados por la OTI.
g. Todo ingreso de mochilas, maletines o bolsos grandes deben ser revisados a la entrada y a la salida de las instalaciones de la ONP.

8.5.5. Seguridad de oficinas, despachos y recursos

La seguridad física para oficinas, despachos y recursos debe considerar lo siguiente:

a. Deberán considerarse los lineamientos señalados en el Reglamento de Seguridad y Salud en el Trabajo de la ONP.
b. Donde sea pertinente, previa evaluación, se deberá instalar equipos con clave de acceso para evitar el acceso a personas no autorizadas.
c. Donde sea aplicable, los edificios o locales deben ser discretos y dar una mínima indicación de su propósito, sin signos obvios, fuera y dentro del edificio, que identifiquen la presencia de actividades de tratamiento de datos e información.

8.5.6. Protección contra amenazas externas y ambientales

a. Todo material combustible y peligroso debe ser almacenado en algún lugar distante de las áreas seguras y zonas de acceso restringido.
b. Las cintas de backup y equipamiento de respaldo será almacenado en ambientes externos fuera de la oficina principal, distante un mínimo de 5 Km. y bajo las condiciones de humedad y temperatura definidas por el fabricante de las cintas.
c. Todos los ambientes de la ONP deben contar con al menos un extintor contra incendios. El número y tipo de extintores, así como la mejor ubicación será coordinado por el equipo de trabajo de Logística.

8.5.7. Trabajo en áreas seguras

a. Se deberá diseñar y aplicar los procedimientos necesarios para la protección física de las instalaciones y pautas para trabajar en áreas seguras.
b. Las áreas donde se procesen información crítica ya sea de característica digital o física deberán contar con la señalización y pautas respectivas de seguridad, de tal forma que el usuario que opere dentro de dichas áreas, tenga el mínimo cuidado posible.
c. Instalaciones como data center, almacén de equipos informáticos, sala de documentación y/o archivos deben contar siempre con un custodio y/o responsable que supervise los trabajos que se realicen en dichas instalaciones. La supervisión del responsable y/o custodio deberá de alguna otra manera evidenciarlo mediante bitácoras o registro de control.

d. No están permitidos los dispositivos de audio, video, fotográfico, de almacenamiento digital, así como algún implemento de carga personal (mochila, bolsos, carteras, etc) en el momento que se acceda a las instalaciones de data center, almacén de equipos informáticos, sala de documentación y/o archivos que procesen y/o almacenen información crítica ya sea de característica física y/o digital, dichos dispositivos e implementos quedarán bajo la debida custodia hasta que se concluya con el trabajo a realizar en la instalaciones mencionadas y posteriormente devueltas a su propietario.

8.5.8. **Zonas de acceso público, carga y descarga.**

a. Se deberán diseñar puntos de acceso para la carga, descarga y acceso público con los controles debidos en zonas donde exista tratamiento de información crítica, de tal manera que se aísle y no se comprometa dichas zonas de tratamiento de información.
b. Para el embarque y recepción de activos de información se debe contar con algún registro que evidencie el estado de tal activo para asegurar la integridad y veracidad de los mismos.
c. La recepción y entrada de activos información debe ser gestionada de acuerdo a lo señalado en la Directiva Gestión Administrativa y de Recursos Humanos vigente.
d. Se deberá informar inmediatamente al custodio inmediato o al Gestor de la Seguridad de la Información cualquier alteración (en todos sus significados) de los activos de información pertenecientes a la ONP.

8.5.9. **Protección y ubicación del equipamiento:**

a. Está prohibido el ingreso o retiro de las instalaciones de la ONP de cualquier equipo de cómputo o de red, salvo autorización expresa que se soporta en los documentos normativos internos vigente a la fecha.
b. Es responsabilidad de la OTI gestionar (registro, traslado, instalación, asignación, mantenimiento, configuración, custodia) los equipos informáticos de propiedad o alquiler de la ONP con la finalidad de proteger su integridad y garantizar su funcionamiento.
c. Se prohíbe que personal no autorizado por la OTI realice alguna actividad como el registro, traslado, instalación, asignación, mantenimiento, configuración y custodia de los equipos informáticos propiedad o alquiler de la ONP.
d. La OTI será la encargada de aprobar y autorizar los requerimientos de hardware de la ONP, de revisar y dar conformidad a los equipos entregados por un contratista, asimismo con los servicios que estén relacionados en forma directa con el hardware de la entidad.
e. El Equipo de Trabajo de Logistica es el responsable de informar a la OTI sobre toda adquisición, alquiler, recepción, evaluación de contratistas de equipos informáticos[4] y de contratistas de servicios que tengan relación con el hardware de la ONP.
f. Es responsabilidad del personal informar a la OTI cualquier evento que afecte la administración de la plataforma tecnológica que brinda servicios para la ONP.

[4] Esta evaluación está referida en el aspecto administrativo y contractual.

g. El Equipo de Trabajo de Logística en coordinación con la OTI mantendrán actualizados los procedimientos de control físico de ingreso y salida de equipos de cómputo de los locales de la ONP.
h. Todos los equipos de cómputo y equipos de red, deben estar en ambientes que posean protección física adecuada, para evitar así la manipulación indebida y robo de los mismos.
i. Las responsabilidades y uso relacionados a los equipos de computación móvil deben estar documentados, detallándose entre otros aspectos los controles de seguridad físicos y las recomendaciones para el uso de estos dispositivos en redes externas.
j. Todo computador portátil de la ONP deberá contar con controles de seguridad física para evitar robos.

8.5.10. **Sistemas e instalaciones de suministros:**

Los equipos críticos como son los servidores centrales, equipos de comunicación de red y equipos de seguridad perimetral deben poseer sistemas redundantes (fuentes de poder, conexiones eléctricas adicionales) y una gestión de energía idónea para minimizar las interrupciones del servicio.

8.5.11. **Protección del cableado eléctrico y de datos:**

El cableado eléctrico y el cableado de datos, deben estar instalados siguiendo las normativas técnicas aplicables para el caso.

8.5.12. **Mantenimiento de los equipos:**

Los equipos deben tener un plan de mantenimiento preventivo periódico. Debe monitorearse el cumplimiento estricto de dichos planes. Si existiera algún equipo que necesite soporte técnico, éste deberá solicitarse a través de la Mesa de Ayuda de Servicios.

8.5.13. **Salida de activos de información fuera de la institución:**

Se debería aplicar los siguientes lineamientos:

a. Debe existir previa autorización evidenciada, para cualquier salida de activos de información sea al interior de la institución o fuera de ella.
b. Se debe de realizar registros para la salida de activos de información fuera de la institución donde se identifique y se registre lo mínimo posible de información, por ejemplo:
   i. Nombre de Activo.
   ii. Tipo de Activo.
   iii. Estado de activo.
   iv. Cantidad
   v. Origen y Destino.
   vi. Fecha y hora
   vii. Motivo
   viii. Datos del responsable del envío, del solicitante y del que autoriza.

c. Todo activo de información que salga de la ONP hacia el exterior debe hacerlo implementando medidas de seguridad de acuerdo al tipo y forma

de transporte, siendo protegidos contra uso no autorizado, mal uso o corrupción durante su transporte, preservando así la confidencialidad, disponibilidad e integridad de la información.

d. Ante la posibilidad de intercambio de información con terceros se debe establecer procedimientos y acuerdos de seguridad formales de intercambio de información.

8.5.14. Seguridad de los equipos y activos fuera de las instituciones.

Se debería aplicar los siguientes lineamientos:

a. Todos los equipos de la ONP que presten servicio en otras instituciones deberán cumplir todas las medidas físicas y lógicas de seguridad pertinentes para su uso correcto y evitar algún robo u alteración de los mismos.
b. Se debe de constatar mediante un documento, la entrega del activo informático de la ONP al usuario solicitante, el cual tiene debe indicar el compromiso a la custodia y uso responsable del activo o se someta a las implicancias pertinentes.

8.5.15. Seguridad en la reutilización, eliminación y retiro de equipos

a. Todos los equipos de almacenamiento de información deben ser revisados con el fin de asegurar que cualquier dato u información y software con licencia haya sido removido o sobrescrito con seguridad, en lugar de utilizar las funciones de borrado estándar, antes de la eliminación, reutilización o retiro.
b. Los dispositivos dañados que contienen información sensible pueden requerir una evaluación para que el propietario de la información determinar si es que deben ser destruidos físicamente en lugar de ser reparados o descartados.
c. Todo el personal que por sus funciones requiera retirar equipos deberá contar con la aprobación y el registro de control correspondiente.
d. El tiempo en que un equipo estará fuera de las instalaciones de la ONP deberá ser especificado al momento de su retiro y su fecha de retorno verificada para asegurar la conformidad.

8.5.16. Equipo informático de usuario desatendido.

a. Se deberán aplicar mecanismos automáticos que permitan el bloqueo de sesión en los equipos de cómputo de la organización cuando no se esté haciendo uso de ellos en un tiempo considerable, a su vez se debe permitir que el mismo propietario lo desbloquee.
b. Los propietarios de los equipos de cómputo no deberán dejar sus estaciones de trabajo desatendidas con sesiones abiertas, debiendo bloquear la sesión cada vez que se moviliza dentro o fuera del área de trabajo.
c. Los usuarios deberán cerrar sesión en cualquier aplicativo que requiera credenciales de autenticación (programas, BD, red y monitoreo) que hayan dejado de usar y no sea requerido.
d. Se deberá bloquear las fotocopiadoras (o proteger de alguna manera del uso no autorizado), a su vez proteger equipos de Fax no atendidos

8.5.17. Puesto de trabajo despejado y Pantallas limpias.

Se debería aplicar los siguientes lineamientos:

a. Guardar bajo llave la información sensible o crítica perteneciente a la institución ya sea un medio físico o que se encuentre almacenada en un medio de almacenamiento extraíble, especialmente cuando no se esté haciendo uso de ella.
b. Retirar inmediatamente la información sensible o confidencial una vez impresa o proceder a su eliminación si en caso ya se cuenta con una copia de respaldo y no se hará uso de ella.
c. En lo posible, se deberá tener el escritorio de la pantalla del computador limpio, consignando únicamente datos necesarios para no mostrar o borrar involuntariamente información importante de la organización.

8.6. LINEAMIENTOS DE SEGURIDAD DE LAS OPERACIONES

8.6.1. Objetivo

Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información. Definir una gestión que permita un balance adecuado entre seguridad y funcionalidad de los servicios de procesamiento para el desarrollo de las actividades de la ONP en forma eficiente y confiable.

8.6.2. Alcance

Este lineamiento aplica a todos los servicios de procesamiento de información y de comunicación que la ONP utiliza en la actualidad, así como cualquier otro que se contrate, adquiera, desarrolle o implemente, sin importar el lugar donde se encuentren los servicios y/o sistemas.

8.6.3. Procedimientos de operación y responsabilidades

a. Las actividades relacionadas con la administración de las operaciones de la ONP deberán ser documentadas, considerando como mínimo los siguientes procedimientos:
   i. Procedimiento de Administración y operación de los sistemas
   ii. Procedimiento de respaldo de información
   iii. Procedimiento de actualización de parches para los servidores
   iv. Procedimiento de monitoreo de la red
   v. Procedimiento de atención de la mesa de ayuda
   vi. Procedimiento de recuperación ante fallas de sistemas
   vii. Procedimiento de revisión de la seguridad de los equipos
   viii. Procedimiento de control de cambios
   ix. Procedimiento de gestión de requerimientos de accesos
   x. Procedimiento de gestión de incidentes

b. Los procedimientos que se documenten deberán especificar las instrucciones necesarias para la ejecución detallada de las tareas.
c. Donde sea técnicamente viable, los sistemas de información deben ser gestionados consistentemente usando los mismos procedimientos, herramientas y recursos.

8.6.4. Gestión de cambios

a. Cualquier cambio en los sistemas de procesamiento debe realizarse a través de un procedimiento de control de cambios, el cual debe contar con los niveles de autorización y registro apropiados.

8.6.5. Gestión de capacidades

a. Se debe contar con un registro actualizado y trazable de toda la infraestructura tecnológica, sea física (equipos de cómputo, comunicaciones y/o red, seguridad perimetral y suministros eléctricos) y lógica (aplicaciones, BD, direcciones Ip y Diagramas de red).
b. Se debe de contar con sistemas que permitan monitorear el performance y el tráfico procesado (throughput[5]) de los Servicios de Tecnologías de Información y los componentes que lo soportan. Estos sistemas deben proporcionar información íntegra y veraz, que permitan tomar decisiones inequívocas y proactivas.
c. Identificados los sistemas de información principales, deben ser monitoreados y optimizados regularmente por el personal del órgano usuario y de la OTI, con el fin de prever problemas de capacidad o situaciones extraordinarias que afecten el desempeño requerido y poder hacer proyecciones de actualizaciones o mejoras. Las actividades de optimización no debe generar ningún riesgo de funcionamiento, ni disminución de la eficiencia y debe realizarse con aprobación de la OTI.

8.6.6. Separación de los recursos para desarrollo, pruebas y producción

a. La OTI es responsable de garantizar la confidencialidad, integridad y disponibilidad de los ambientes de desarrollo, pruebas y producción. Estas actividades están relacionadas con la administración de procesos, de redes, de correo electrónico, de pases a producción de desarrollos y cambios en los sistemas, planes de respaldo, planes de recuperación y otras actividades de acuerdo al MOF de la ONP.
b. Está prohibido que personal no autorizado por la OTI, realice actividades de operación de los recursos de los ambientes de desarrollo, pruebas y producción.
c. Los ambientes de desarrollo, pruebas y de producción deberán estar debidamente aislados, con el fin de reducir los riesgos de los accesos o cambios no autorizados. En el caso de que el aislamiento físico no sea posible, se tomarán las medidas adecuadas, a nivel lógico, para minimizar la posibilidad de riesgos sobre los sistemas de producción.
d. El acceso a los ambientes de desarrollo, prueba y producción deberá ser restringido sólo para personal autorizado.
e. Los ambientes de prueba no deberán ser utilizados como ambientes de desarrollo y viceversa.
f. Los usuarios que almacenen información en los servidores que soportan los ambientes de desarrollo y pruebas, deberán clasificar la información para efectuar la conversión respectiva desde los ambientes de producción a dichos ambientes.

[5] Se refiere al volumen de trabajo o de información neto que fluye a través de un sistema, como puede ser una red de computadoras

g. La sincronización de los ambientes de prueba y desarrollo con la información de los ambientes de producción, deberá ser ejecutada previa aprobación y coordinación con la OTI.
h. Se deberán implementar mecanismos de seguridad lógica y física para los manejadores de base de datos, servidores de aplicaciones e infraestructura física y lógica que soporte los ambientes de desarrollo, prueba y producción.

8.6.7. Protección contra código malicioso

a. Se prohíbe la instalación de programas o aplicaciones en cualquier componente conectado a la red de la ONP, sean estaciones de trabajo, computadoras portátiles, servidores, etc. Esta función la debe realizar únicamente el personal autorizado por la OTI o por personal autorizado por OTI.
b. El Equipo de Trabajo de Administración de Plataformas y Redes deberá coordinar la realización de revisiones periódicas del software instalado en la red. La presencia de cualquier software no autorizado deberá ser investigada y removida.
c. Según factibilidad técnica todos los servidores y estaciones de trabajo en la red de la ONP deberán tener instalado un software de protección contra código malicioso que cuente con un sistema de actualización vigente.
d. Se deberá implementar un sistema de prevención de intrusiones de red que proteja de manera transparente a los servidores principales.
e. Los planes de contingencia tecnológica, deberán considerar las acciones pertinentes para recuperarse de los ataques de virus, incluyendo los datos y software necesarios de respaldo y las disposiciones para la recuperación.
f. Se deberá prevenir la introducción de código malicioso durante el mantenimiento y los procedimientos de emergencia, ya que estos pueden pasar controles normales de protección y exponer los recursos de la ONP.
g. Antes de conectar a la red de la ONP dispositivos externos, como CD/DVD, dispositivos de almacenamiento USB, discos duros externos y otros similares, se deberá verificar que estos no se encuentren infectados con virus.
h. Como medida de mitigación contra virus se deberá inactivar los puertos USB, y unidades de CD/DVD. Como correo electrónico externo y acceso a internet, las excepciones serán aprobadas y coordinadas con la OTI.
i. Como medida de excepción, en relación a lo señalado en el literal precedente, se deberá desactivar el uso de la reproducción automática para todos los medios y dispositivos (dispositivos USB, CD/DVD, Blu-ray Disc).

8.6.8. Medidas y controles contra código móvil

a. Para los casos en que se aplique el uso de código móvil, se deberá coordinar con la OTI las labores a ejecutar, teniendo presente las siguientes acciones mínimas para proteger a la institución contra acciones no autorizadas de códigos móviles:
   i. Ejecutar el código móvil en un ambiente lógico aislado.
   ii. Bloquear cualquier uso de código móvil.

iii. Bloquear el recibo de código móvil.
iv. Activar medidas técnicas cuando estén disponibles en un sistema específico para asegurar que el código móvil está controlado.
v. Controlar los recursos disponibles al acceso de código móvil.

8.6.9. Gestión de respaldo y recuperación

a. La información, sistemas y programas de la ONP, deberán contar con copias de respaldo actualizadas y debiéndose realizar pruebas regulares de restauración. La OTI aplicará los mecanismos técnicos para este fin.
b. Al menos una copia de respaldo de los datos, sistemas y programas debe almacenarse fuera de las oficinas principales.
c. El personal no debe almacenar información catalogada como **reservada o confidencial**, en los discos duros de las computadoras personales o portátiles asignadas para sus labores. Las excepciones deben ser solicitadas y serán evaluadas por la OTI.

8.6.10. Registro y gestión de eventos de Actividad

a. La red de la ONP debe contar con la posibilidad de generar registros de auditorías de las actividades de los usuarios. Las excepciones y eventos de seguridad de la información deben ser almacenados con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de accesos.

   Los registros deben incluir por lo menos:
   i. Nombre del usuario
   ii. Fechas, horas de los eventos
   iii. Registro de entrada y salida del sistema
   iv. Identificación del Terminal o estación origen

b. Todos los equipos de seguridad y de la red, deberán contar con algún sistema de registros de eventos de seguridad que permita identificar al menos el origen, destino y tipo de tráfico cursado a través del equipo.
c. La OTI establecerá los procedimientos de correlación de los eventos de seguridad.
d. La OTI supervisará que los servicios de información administrados por un tercero cuenten con mecanismos para el monitoreo de la seguridad de la información.
e. La OTI analizará la implementación de controles especiales para resguardar la confidencialidad e integridad de la información cuando ésta pasa por redes públicas.
f. Los trabajos de mantenimiento de los sistemas, que involucren la seguridad de los mismos, deberán ser coordinados con el Gestor de Seguridad de la Información, describiendo obligatoriamente el riesgo asociado al cambio y el procedimiento de retorno al estado anterior.
g. Los requerimientos de seguridad de los sistemas principales de la ONP deberán estar identificados. Se deberán definir el o los controles de seguridad para alcanzar estos requerimientos y monitorear su efectividad.

8.6.11. Protección de la Información de los Registros

a. La OTI debe asegurarse que todos los dispositivos con información de la ONP, previamente identificada por el Gestor de Seguridad de la Información, deberán ser eliminados de manera segura cuando ya no sean utilizados.
b. La OTI establecerá los mecanismos para el manejo y almacenamiento adecuado de los medios removibles que guarden copias de respaldo.

8.6.12. Registros de actividad del Administrador y Operador

a. La OTI es responsable de definir las funciones del personal técnico y el alcance de su administración y operación, así como mantener la documentación relacionada al activo tecnológico administrado, indicando los privilegios necesarios.
b. Se deben mantener registros de auditoria en relación a los activos tecnológicos de la institución, mediante bitácoras, checklist u otro método de seguimiento de las actividades realizadas.
c. En los sistemas tecnológicos (equipos de cómputo, de red, de seguridad perimetral, de aplicaciones y BD), se deberán habilitar las opciones de auditoria de sistemas.
d. Los registros de auditoria de los sistemas tecnológicos, bitácoras, checklist u otros, deberán estar custodiado lógica y/o físicamente en lugares seguros.

8.6.13. Sincronización de Relojes.

a. Se deberán implementar sistemas centralizados y unificados concernientes al tiempo y zona horaria, en el cual todos los sistemas tecnológicos operen y se comuniquen al mismo tiempo, sincronizadamente y verazmente, lo que permitirá tomar decisiones en tiempo real y analizar tendencias de manera inequivoca.

8.6.14. Instalación del software en sistemas de producción.

a. Se deberán identificar los sistemas de información principales de la organización.
b. Las actualizaciones de Sistemas Operativos, librerías y diversas aplicaciones, deberán ser gestionadas por el Equipo de Trabajo de Administración de Plataformas y Redes. La OTI deberá definir los criterios para la aceptación de nuevos sistemas o nuevas versiones antes de su puesta en producción. En forma mínima se deberá contar con:
    i. Manuales de operación y administración
    ii. Evaluación de riesgos
    iii. Capacitación
    iv. Planes de contingencia

8.6.15. Gestión de las vulnerabilidades técnicas

a. La OTI deberá establecer mecanismos para gestionar las vulnerabilidades técnicas de las aplicaciones, gestionando la evaluación de riesgos, impacto y probabilidades de ocurrencia.

b. La implementación de las modificaciones de una aplicación para corregirla o alterarla por algún motivo (parches de sistemas) deberá ser evaluada y probada antes de ser aplicada en los sistemas de producción. Estas actividades deberán ser ejecutadas y supervisadas por la OTI, según corresponda.
c. La OTI establecerá la programación de revisiones de vulnerabilidades regulares, como mínimo una vez al año; y realizará revisiones extraordinarias cuando estas sean solicitadas o el caso lo amerite.

8.6.16. Restricciones en la instalación de software.

a. La OTI deberá establecer los mecanismos para permitir que tipos de software se deban de instalar en los equipos de la ONP.
b. La OTI deberá aplicar las restricciones y/o privilegios pertinentes a los usuarios en cuanto al tipo de software que requieran y dependiendo de las funciones que realicen, esto será canalizado hacia un personal técnico

8.6.17. Controles de Auditoria de los sistemas de información.

a. La OTI deberá planificar y acordar los requisitos y las actividades de auditoría que involucren la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.

8.6.18. Monitoreo

a. La red de la ONP deberá contar con la posibilidad de generar registros de auditorías de las actividades de los usuarios. Las excepciones y eventos de seguridad de la información deberán ser almacenados con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de accesos.

   Los registros deberán incluir por lo menos:
   i. Nombre del usuario
   ii. Fechas, horas de los eventos
   iii. Registro de entrada y salida del sistema
   iv. Identificación del Terminal o estación origen

b. Los archivos que contengan registros de eventos deberán estar protegidos. Asimismo, el acceso a dichos archivos deberá estar restringido sólo al personal de seguridad de la información. Sólo con autorización por escrito del Jefe de la OTI, podrá ser suministrado.
c. Las fallas reportadas por los usuarios o administradores de sistemas deberán ser registradas y comunicadas siguiendo los mecanismos que se establezcan para tal fin.

8.7. LINEAMIENTOS DE SEGURIDAD DE LAS COMUNICACIONES

8.7.1. Objetivo

Asegurar que la información reciba el nivel de protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo según su importancia para la organización.

8.7.2. Alcance

Este lineamiento aplica a todos los servicios de comunicación que la ONP utiliza en la actualidad, así como cualquier otro que se contrate, adquiera, desarrolle o implemente, sin importar el lugar donde se encuentren los servicios y/o sistemas.

8.7.3. Gestión de Seguridad de la Red

a. **Controles de RED**
   i. Las redes deben gestionarse y controlarse para proteger la información en los sistemas y aplicaciones.
   ii. Los sistemas en la red deben ser restrictivos en su mayoría, deben solicitar autenticación y registro.
   iii. Los controles deberán hacerse en todas las capas lógicas de la red.

b. **Seguridad de los servicios de la RED:**
   i. Todos los servicios de red deberán contemplar mecanismos de seguridad, niveles de servicios y requisitos de gestión identificados.

c. **Separación en las redes**:
   i. Las redes de comunicación deberán ser segmentadas por criterios de uso, usuario final, dispositivos conectados, etc., de modo que se puedan gestionar adecuadamente las mismas.
   ii. Las comunicaciones inalámbricas deben realizarse utilizando como mínimo un mecanismo de autenticación y encriptación.
   iii. Queda prohibida la conexión a la red de datos y de telefonía de la ONP, de cualquier dispositivo móvil que pertenezca al personal.

8.7.4. Transferencia de Información

a. **Lineamientos y procedimientos de transferencia de información**
   i. Se deberán implementar mecanismos que regulen los diferentes tipos de transferencia de datos, ya sea a través de la red de comunicaciones o a través de dispositivos de almacenamiento.
   ii. Se deberán establecer controles de mensajería física para que durante el transporte se verifique que la información no fue accedida por alguien no autorizado.
   iii. Se deberán establecer protocolos seguros para el tránsito de la información hacia la empresa que va a recibir alguna información.

b. **Acuerdos sobre transferencia de información**
   i. El propietario de la información en coordinación con la OTI establecerá criterios de seguridad para el intercambio de

información, utilizando medio seguros, lugares seguros, tiempos y periodos apropiados.

c. **Mensajería electrónica**
   i. Se deberán mantener actualizados los documentos normativos referidos al uso los servicios de mensajería electrónica, de modo que se preserve la confidencialidad de la información de acuerdo al nivel definido.
   ii. La OTI es el órgano encargado de la administración del correo electrónico de la entidad asegurando su continuidad operativa, manteniendo actualizadas las cuentas de correo, tomando las medidas de seguridad contra virus u otros y controlando el uso indebido de las cuentas de correos por parte del personal estableciendo las normas y/o procedimientos que regulen este Lineamiento, disponiéndose los controles con herramientas informáticas que garanticen el cumplimiento del mismo.

d. **Acuerdos de confidencialidad:**
   i. La OTI revisará periódicamente los acuerdos de confidencialidad asociados a la transferencia de información en los diferentes servicios.

8.8. LINEAMIENTOS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

8.8.1. Objetivo

Asegurar que todos los sistemas de información actuales y nuevos incluyan requerimientos de seguridad para proteger la confidencialidad, integridad y disponibilidad de los datos que manejan.

8.8.2. Alcance

Este grupo de lineamientos se aplica a todos los sistemas de información actuales y futuros bajo la administración de la ONP, bajo la supervisión de la OTI.

8.8.3. Requerimientos de seguridad en las aplicaciones

a. La seguridad deberá ser considerada en la fase de definición de requerimientos de una nueva aplicación, es decir antes de la adquisición de un sistema nuevo.
b. La OTI, deberá evaluar los riesgos en el desarrollo, implementación y mantenimiento de las nuevas aplicaciones respecto a los sistemas de información actuales para determinar algún control de seguridad necesario.
c. Los requerimientos de seguridad en las aplicaciones estarán orientados al cumplimiento de estándares, normas técnicas y buenas prácticas en el desarrollo de sistemas.

8.8.4. Aseguramiento de servicios de aplicación en redes públicas

a. Se deberá asegurar y fortalecer la publicación de servicios externos, para prevalecer la confidencialidad, disponibilidad e integridad de la información.
b. Las aplicaciones publicadas por la ONP deberán protegerse contra todo tipo de ataques externos, evitando así la interrupción y denegación de los servicios

8.8.5. Proteger las transacciones de servicios de aplicaciones

a. Se deberán aplicar las mejores prácticas tecnológicas de enrutamiento, aislamiento, denegación y comunicaciones encriptadas para las transacciones de servicios de aplicaciones de la ONP.
b. Las comunicaciones entre aplicaciones y la consulta del usuario a la aplicación deberán realizarse bajo protocolos de comunicación segura. De ser demasiado restrictiva y que no se dé una comunicación fluida, deberá de ser analizada por la OTI y si en caso amerite afinar ciertos parámetros, se tomará ciertas consideraciones del caso.

8.8.6. Lineamiento de desarrollo seguro

a. La OTI deberá establecer normas y lineamientos para el desarrollo de software y así como para la aplicación de sistemas a los desarrollos dentro de la organización.
b. La OTI definirá los estándares de programación sobre los cuales se deberán incluir buenas prácticas de codificación para disminuir las vulnerabilidades de seguridad.
c. La OTI definirá un estándar para el tratamiento de los módulos de administración de accesos y perfiles de los sistemas.

8.8.7. Procedimientos de control de cambios del sistema

a. Se debe mantener actualizado la normativa referida a la gestión de cambios en los sistemas y aplicaciones de la ONP. El procedimiento deberá incluir como mínimo:
   i. Lista de personas autorizadas a solicitar cambios
   ii. Tipos de cambios (menor, mayor)
   iii. Niveles de autorización de los cambios
   iv. Actualización de documentación
   v. Control de Versiones

8.8.8. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

a. La OTI definirá guías y procedimientos para la instalación y actualización del software operativo y de las aplicaciones de la ONP. Estas guías y procedimientos deberán ser usadas por el personal autorizado para dicho fin.
b. Luego de la actualización de algún sistema, la OTI coordinará una revisión técnica de los resultados para medir el impacto de los cambios en la ONP. El resultado será documentado como parte de la Gestión de la Seguridad y será comunicado a las instancias correspondientes.

V° B° JENNIFER AYLLÓN BULNES ONP

c. La actualización de los componentes de cualquier aplicación o del sistema operativo será realizada únicamente por el personal autorizado de la OTI siguiendo los mecanismos establecidos en los procesos de la OTI.

8.8.9. Restricciones de cambios en los paquetes de software

a. Todos los programas fuente, incluidos los comandos de acceso directo a las bases de datos y servidores de aplicaciones y sus correspondientes librerías que conformen un sistema de información, deberán tener un acceso restringido al personal de la OTI. Está prohibida su divulgación fuera de la OTI, salvo permiso expreso de dicho órgano y/o por razones de servicios de soporte de contratistas externos.

8.8.10. Principios de ingeniería de un sistema seguro

a. La OTI deberá establecer y aplicar metodologías, principios, estándares y/o mejores prácticas, donde se permita analizar, diseñar, desarrollar e implementar sistemas seguros.

8.8.11. Entorno de desarrollo seguro

a. La OTI deberá implementar y proporcionar espacios e infraestructura segura para desarrollar, testear, desplegar e integrar sistemas a todo lo largo del ciclo de vida de desarrollo de software.
b. Los entornos de desarrollo deberán apoyarse y tomar en cuenta las medidas de seguridad ya indicadas en los lineamientos desarrollados en la presente directiva vinculados a la gestión de accesos, copias de seguridad, comunicaciones seguras, registro y supervisión.

8.8.12. Desarrollo externalizado

a. En caso que el desarrollo de un sistema, aplicación o algún módulo, no sea realizado por personal de la ONP, para efectos de su implementación, la OTI tomará las medidas de protección respecto a la confidencialidad, propiedad del código fuente y derechos de autor a través de los canales correspondientes.

8.8.13. Pruebas de funcionalidad durante el desarrollo de los sistemas

a. El ingreso de datos debe ser validado por la aplicación para asegurar que sea un dato correcto y consistente con la información a procesar.
b. En caso, el ingreso de datos sea a través de otras aplicaciones, deben implementarse chequeos de validación en la transmisión o en el procesamiento interno de la aplicación para detectar cualquier corrupción de la información.
c. La salida de datos en una aplicación también debe ser validada, para asegurar que la información sea correcta y pertinente para el usuario.

8.8.14. Pruebas de Aceptación

a. Cualquier cambio mayor sólo deberá ser implementado si se ha pasado por un análisis previo, que incluye una evaluación de los riesgos, tener

documentado un plan detallado de pruebas y un plan de restauración a la condición anterior.

8.8.15. Protección de Datos de Pruebas

a. Los datos e información de producción no deben ser copiados en los entornos de desarrollo y prueba. La información de los ambientes de desarrollo y prueba deberán ser transformada lógica y coherentemente para no exponer la información del ambiente de producción.
b. Los sistemas de información, deberán exhibir mensajes de identificación apropiados para identificar si los usuarios han ingresado a los ambientes de desarrollo prueba o producción, con el fin de reducir el riesgo por error.
c. Los datos de pruebas de los ambientes de desarrollo, pruebas y producción deben ser protegidos y controlados. Los datos no pueden ser utilizados fuera de la ONP, salvo autorización expresa de la jefatura de la OTI, y coordinado previamente con el Usuario Líder de las aplicaciones.

8.9. LINEAMIENTOS DE RELACIONES CON TERCEROS

8.9.1. Objetivo

Lineamientos para asegurar la protección de los activos de información de la organización a que tienen accesos terceros.

8.9.2. Alcance

a. Este lineamiento aplica a todos los servicios de comunicación que la ONP utiliza en la actualidad y exista la necesidad de controles criptográficos, así como cualquier servicio que se contrate, adquiera, desarrolle o implemente, sin importar el lugar donde se encuentren los servicios y/o sistemas.

8.9.3. Lineamientos Seguridad de Información con las relaciones con el proveedor

a. Los órganos y equipos de trabajo de la ONP y la OTI deberá establecer disposiciones en materia de seguridad de información relacionadas a los servicios con terceros, a fin de mitigar los riesgos de seguridad de manera que estos sean brindados de manera segura y eficiente.
b. Cuando el negocio requiera el acceso de terceros, se deberá realizar una evaluación del riesgo para determinar sus implicaciones sobre la seguridad y las medidas de control que se requieren. Estas medidas de control deberían incluirse en el contrato con la tercera parte.

8.9.4. Gestión de la prestación del servicio de terceros

a. En los términos de referencia de los servicios deben especificarse las obligaciones en el marco de la seguridad de la información que debe cumplir el tercero, así como la responsabilidad asociada a la implementación de los controles relacionados.

b. La ONP se reserva el derecho de revisar regularmente los registros de auditoria y solicitar reportes de seguridad para verificar el cumplimiento de los acuerdos de los contratos respecto a la protección de la información.
c. El personal de la OTI, en coordinación con el Gestor de Seguridad de la Información, en función al riesgo que podría generar para los sistemas en la ONP, evaluará la procedencia de cualquier cambio a realizar por el contratista en la prestación del servicio (equipos, software, sistemas, personal o condiciones de operación).
d. Los incidentes de seguridad ocurridos durante la prestación de servicios por terceros deberán ser comunicados al Gestor de Seguridad de la Información para el tratamiento correspondiente según el nivel de sensibilidad.

8.10. LINEAMIENTOS DE GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE INFORMACION

8.10.1. Objetivo

Asegurar que todos los eventos o debilidades asociados con la seguridad de información, sean comunicados oportunamente por el personal afectado a los responsables de seguridad.

8.10.2. Alcance

Este lineamiento abarca a todo dato y/o información utilizada en la ONP para el desarrollo de sus actividades y es aplicable, obligatoriamente, a todo el personal de servicios involucrados en la utilización de la información, y a los recursos de información que los soportan.

8.10.3. Gestión de incidentes de seguridad de la información y mejoras

a. Las acciones a seguir, responsabilidades y escalamientos que se deriven de la atención de un incidente de seguridad deberán ser definidos en procedimientos formales.
b. La OTI definirá las acciones conducentes para llevar el control correspondiente de los incidentes de seguridad de la información en la ONP.
c. Los controles deberán incluir las responsabilidades sobre la gestión y atención de los incidentes.
d. El personal está en la obligación de reportar lo más pronto posible cualquier evento o debilidad de seguridad en los activos.
e. La gestión de incidentes de seguridad de la información debe incluir, como mínimo, las siguientes actividades:
   i. Recepción y registro del incidente
   ii. Clasificación y valoración del impacto
   iii. Priorización de la atención
   iv. Escalamiento del incidente
   v. Resolución del incidente
   vi. Gestión de problemas
   vii. Elaboración de informe

f. La OTI deberá implementar protocolos de acción respecto a la identificación, recolección, adquisición y preservación de la evidencia en previsión de tomar alguna acción legal o administrativa contra el personal involucrado. Estas definiciones deberán realizarse con el apoyo de la ORH y la OAJ. El resguardo de esta evidencia será derivado a la OAJ cuando la investigación lo amerite.
g. Se debe mantener y usar una base de conocimiento con información relacionada sobre nuevas vulnerabilidades, información de los servicios habilitados y experiencias con incidentes anteriores.
h. Cuando un incidente de seguridad involucre la vulneración de datos personales, se deberá informar al titular de datos personales afectado sobre el detalle del mismo y las acciones correctivas efectuadas, acorde a lo dispuesto en la Ley de Protección de Datos Personales.

8.11. LINEAMIENTOS DE SEGURIDAD DE LA INFORMACION PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

8.11.1. Objetivos

a. Responder ante las interrupciones de las actividades de la ONP y proteger los procesos críticos ante los efectos de una falla mayor por problemas relacionados a la seguridad de la información.
b. Minimizar el impacto en la organización y recuperarse de una pérdida de los activos de información principales de información por un desastre (desastre natural, incendio, inundación, acciones deliberadas, etc.), asegurando la recuperación en tiempos tolerables para la ONP.

8.11.2. Alcance

Este lineamiento aplica a todos los sistemas de información que soportan a los procesos críticos dentro del Centro de Cómputo principal de la ONP.

8.11.3. Información general

a. Los planes para la continuidad de las operaciones de una organización son los siguientes, siendo el más importante para el caso de la ONP el Plan de Recuperación ante Desastres.
   i. **Plan de Contingencia Tecnológica**: planes orientados a recuperar componentes específicos de la red, por ejemplo planes de contingencia de comunicaciones, de servidores, de red LAN, etc.
   ii. **Plan de Recuperación ante Desastres**: su objetivo es la recuperación de los principales activos de información que soportan a los procesos críticos de la ONP en un sitio externo de respaldo ante la eventualidad de un desastre mayor. Su alcance comprende lo referido a Tecnologías de la Información.
   iii. **Plan de Continuidad Operativa:** incluye la recuperación de las actividades principales de la ONP, identificando los requerimientos mínimos en términos de logística, personal y sistemas de información. En el siguiente gráfico se muestra la jerarquía de estos planes.

8.11.4. Lineamiento Continuidad de la Seguridad de la Información

a. Todos los procesos de la ONP, deben contener un análisis de continuidad ante una contingencia tecnológica, incluyendo los requerimientos de seguridad respecto a la protección de la confidencialidad, integridad y sobretodo de la disponibilidad de su información, lo cual debe estar descrito en el manual del proceso.
b. Los órganos y equipos de trabajo de la ONP deberán identificar todos los activos de información que soportan a los procesos críticos, así como su impacto en las operaciones, ante la eventualidad de su indisponibilidad más allá de los tiempos tolerables para la ONP.
c. Los órganos y equipos de trabajo de la ONP informarán sus requerimientos de respaldo. Los órganos y equipos, según su competencia, evaluarán la factibilidad de la atención de los requerimientos a través de equipamiento redundante, contratos de mantenimiento y de soporte técnico, Centro de Cómputo alterno, pólizas de seguro, fondo de respaldo financiero y logístico, así como protección del personal como medidas preventivas ante la eventualidad de un desastre mayor que imposibilite las operaciones dentro de las oficinas principales. Como resultado se elaborará un informe técnico con las recomendaciones para su evaluación correspondiente.
d. El Gestor de Seguridad de la Información, identificará los posibles eventos que puedan causar una indisponibilidad de los servicios Tecnologías de Información, a través de un análisis de impacto, evaluando su probabilidad e impacto y las consecuencias para la seguridad de la información.
e. Se manejarán estándares para desarrollar, mantener y documentar los planes de contingencia tecnológica como también los planes de recuperación ante desastres.
f. En el desarrollo de los planes de contingencia, de recuperación ante desastres se identificarán expresamente:
    i. Los activos de información protegidos por el plan
    ii. Los responsables de activar, ejecutar y restaurar
    iii. Los procedimientos para la activación, ejecución y finalización del plan
    iv. Los procedimientos operativos de recuperación
    v. Las pruebas y planes de mejora
g. Ante un desastre y según las responsabilidades asignadas en los planes de contingencia tecnológica y recuperación ante desastres, el personal, haciendo uso de sus habilidades, está en la obligación de asistir a los

procesos de recuperación y restauración de las actividades normales de la ONP.

h. Los responsables de los órganos de la ONP deberán incluir en los términos de referencia, para cada uno de los servicios contratados, las acciones a realizar y el compromiso del servicio en caso de un desastre.
i. Los responsables de los órganos de la ONP, según corresponda, supervisaran que los planes de contingencia tecnológica de componentes de la red, los planes de recuperación ante desastres y el plan de continuidad de las operaciones se revisen cada año para garantizar su vigencia.
j. La OTI definirá la estrategia de pruebas anual de los planes, entre las cuales pueden existir:
    i. Pruebas de componentes tecnológicos (servidores, sistemas, redes, etc.).
    ii. Pruebas de escritorio (revisiones de los planes en reunión de focus group).
    iii. Pruebas reales (pruebas de todos los componentes).

En cada prueba se redactará un informe para la actualización y mejora de los planes vigentes, haciendo de conocimiento a la Oficina de Gestión de Riesgos.

8.11.5. Redundancias

a. Los órganos que sean responsables del tratamiento y procesamiento de la información, deberán de analizar y planificar la implementación de sistemas, infraestructura, locaciones, facilidades, insumos, y recursos humanos que soporten, prevean y conmuten de la manera más eficaz y que no contengan puntos de falla y así preservar la disponibilidad y continuidad de las instalaciones de procesamiento de información.
b. Los sistemas, infraestructura y locaciones redundantes no deben de estar ubicados físicamente en el mismo espacio, área, edificio o perímetro de 400 mt. lineales. Se deben establecer lugares inclusive fuera de la misma jurisdicción que cumplan con estándares de seguridad (físico y lógico) y calidad.

8.12. LINEAMIENTOS DE CUMPLIMIENTO

8.12.1. Objetivo

a. Asegurar el cumplimiento de los lineamientos y normativa de seguridad de información en la ONP.
b. Establecer lineamientos de seguridad para la protección de datos personales recolectados, tratados y/o almacenados por la ONP en cumplimiento de sus funciones.
c. Cumplir con lo dispuesto en la Ley N° 29733 – Ley de Protección de Datos Personales y su Reglamento.

8.12.2. Alcance

a. Está comprendido en el alcance de este lineamiento todo el personal que por algún motivo de actividad laboral tenga acceso a los activos de información de la ONP. Se incluyen también los activos de información

que requieran contratos de licenciamiento de uso de activos de información y procesos por parte de terceros.

b. Este lineamiento también aplica para al tratamiento de datos personales contenidos o destinados a ser contenidos en bancos de datos personales de la ONP, cuyo tratamiento se realiza en el territorio nacional.

8.12.3. Cumplimiento de los requisitos legales y contractuales

a. La infraestructura de información (sistemas, lineamientos, procesos, etc.) sólo deberá ser usada para los propósitos, fines y objetivos de la ONP.
b. El personal se somete a las medidas administrativas y acciones legales, conforme a lo que establece el Reglamento Interno para los Servidores de la ONP y el marco contractual para los contratistas que se deriven del incumplimiento de las disposiciones establecidas en el presente documento.
c. La ORH deberá promover la concientización para el cumplimiento de la Ley de derechos de autor y propiedad intelectual, respetando así las leyes vigentes y decretos legislativos.
d. La OTI deberá de aplicar controles sobre las instalaciones de software autorizado y productos bajo licencia, asimismo mantendrá los documentos que acrediten la propiedad de licencias como los manuales, llevando el control respectivo.
e. La OTI deberá establecer los lineamientos de mantenimiento y de eliminación de software, así como de su transferencia a terceros.

8.12.4. Protección de Datos y Privacidad de la Información Personal

a. Principios rectores aplicables al tratamiento de datos personales

En la ONP, la protección de los datos de carácter personal se rige por una serie de principios rectores que serán la base de los procesos internos relacionados al tratamiento de los datos personales.

i. **Consentimiento**
El tratamiento de datos personales en la ONP, sólo puede hacerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos, tratados o divulgados sin autorización del titular salvo mandato legal o judicial que supla el consentimiento del titular de los datos personales.

ii. **Finalidad**
La recolección, tratamiento y/o almacenamiento de datos personales en la ONP obedece a una finalidad determinada y legítima acorde con sus funciones, la cual es informada de manera precisa, concreta y previa al titular de los datos para que éste exprese su consentimiento informado.

iii. **Legalidad**
En la ONP, el tratamiento de los datos personales se hace conforme a lo establecido en la Ley N°29733 – Ley de Protección de Datos Personales y su Reglamento.

iv. **Calidad**
Es de preocupación para la ONP, que los datos personales que recolecta sean veraces, completos, comprobables, comprensibles y

actualizados. Está prohibido el tratamiento de datos parciales o incompletos.

v. **Proporcionalidad**
El tratamiento de datos personales en la ONP, se realizará de acuerdo a los lineamientos normativos y se delimita exclusivamente por la finalidad que ameritó su recolección.

vi. **Seguridad**
La ONP adoptará medidas de seguridad para garantizar la confidencialidad, integridad y disponibilidad de los datos personales. Estas medidas están implementadas de acuerdo al tratamiento que reciben los datos y al nivel de sensibilidad que presentan.

vii. **Disponibilidad de recurso**
La ONP garantizará que los titulares de los datos personales dispongan de las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.

b. **Derechos de los titulares de los datos personales tratados en la ONP**

La ONP realizará el tratamiento de datos personales que provienen de diversas categorías de titulares, tales como:

I. Personal institucional
II. Contratistas (Bienes y servicios)
III. Clientes (Asegurados y Pensionistas)
IV. Ciudadanía en general

Dichos titulares de datos personales podrán ejercer los siguientes derechos, siendo prioridad de la ONP su cumplimiento:

i. **Derecho de Información**
El titular de los datos personales tiene derecho a ser informado, previamente a su recolección, sobre los siguientes aspectos respecto a sus datos:
- Finalidad para la cual son recolectados
- Banco de datos personales que los almacenará
- Identidad del titular del banco de datos y el encargado del tratamiento, de presentarse ambos roles
- El carácter obligatorio o facultativo de los datos a ser presentados
- Mecanismos de transferencia de los datos, de ser el caso
- Tiempos de almacenamiento
- Posibilidad de ejercer los derechos que la ley concede respecto a los datos registrados

ii. **Derecho de acceso**
Es el derecho de solicitar toda la información concerniente a sus propios datos personales, al tratamiento aplicado a los mismos, a la finalidad de recolección, a la ubicación de los bancos donde se almacena y las comunicaciones realizadas respecto a ellos.

iii. **Derecho de actualización, inclusión, rectificación y supresión**
El titular de los datos personales tiene derecho a la actualización, inclusión y rectificación de sus datos, cuando estos sean parcial o

totalmente inexactos, incompletos o cuando se haya incurrido en error o falsedad.
En el caso de la supresión de los datos personales, la ONP se somete a lo dispuesto en el artículo 21 de la Ley N° 27806 – Ley de Transparencia y Acceso a la Información Pública y su modificatoria.

iv. **Derecho de oposición**
El titular de los datos personales puede oponerse al tratamiento de los mismos, siempre que por ley no se disponga lo contrario y existan motivos legítimos y fundados.

v. **Derecho al tratamiento objetivo**
El titular de datos personales tiene derecho a no verse sometido a una decisión con efectos jurídicos sobre él, sustentada únicamente en un tratamiento de datos personales destinado a evaluar determinados aspectos de su personalidad o conducta, salvo que ello ocurra en el marco de una negociación, celebración o ejecución de un contrato o en los casos de evaluación con fines de incorporación laboral a la ONP, de acuerdo a ley.

vi. **Derecho a la tutela**
La ONP garantiza la atención a los titulares de los datos personales ante cualquier requerimiento, en ejercicio de los derechos contemplados en la Ley N° 29733 – Ley de Protección de Datos Personales y su Reglamento. Asimismo, la ONP reconoce a la Dirección General de Protección de Datos Personales del Ministerio de Justicia, como la autoridad máxima en materia de protección de datos personales a nivel nacional y se somete a las disposiciones que ésta dictamine conforme a ley.

c. **Limitaciones para el ejercicio de los derechos**

La ONP se reserva el derecho de denegar al titular de datos personales los derechos de acceso, supresión y oposición ante los siguientes escenarios:

i. Protección de derechos e intereses de terceros
ii. Acciones judiciales o administrativas vinculadas al cumplimiento de obligaciones tributarias o previsionales
iii. Investigaciones penales
iv. Verificación de infracciones administrativas
v. Cuando la ley lo disponga

d. **Disposiciones de la ONP respecto a los roles en la protección de datos personales**

La ONP, enmarcada en el cumplimiento de la legislación vigente en materia de protección de datos personales, define dos roles: El Titular del banco de datos personales, el responsable del tratamiento.

Según el rol determinado, la ONP velará por el cumplimiento de las siguientes disposiciones:

I. **Titular del banco de datos personales**
Asumido por la ONP como entidad pública, tiene las siguientes obligaciones:

a. Informar oportunamente al titular de datos personales sobre la finalidad de la recolección y los derechos que le asisten, salvo las excepciones establecidas por ley.
b. Almacenar los datos personales de manera que se garantice al titular de datos personales, en todo momento, el pleno y efectivo ejercicio del derecho de hábeas data dentro de los plazos establecidos por ley.
c. Recopilar datos personales que sean actualizados, necesarios, pertinentes y adecuados, con relación a finalidades determinadas, explícitas y lícitas para las que se hayan obtenido.
d. No recopilar datos personales por medios fraudulentos, desleales o ilícitos.
e. Solicitar y conservar, según lo estipulado en la legislación vigente, copia y/o evidencia del consentimiento otorgado por el titular de datos personales.
f. Suprimir y sustituir o, en su caso, completar los datos personales objeto de tratamiento cuando tenga conocimiento de su carácter inexacto o incompleto, sin perjuicio de los derechos del titular al respecto.
g. Velar porque que los bancos de datos personales sean tratados bajo efectivas medidas de seguridad para impedir su adulteración, pérdida o acceso no autorizado.
h. Informar oportunamente al órgano delegado para el tratamiento correspondiente, las rectificaciones realizadas sobre los datos personales para que se ejecuten los ajustes pertinentes.
i. Exigir al órgano delegado para el tratamiento, en todo momento, el respeto de las condiciones de seguridad y privacidad de la información del titular de datos personales.
j. Auditar periódicamente el cumplimiento de la Ley N° 29733 – Ley de Protección de Datos Personales y su Reglamento, por parte de los destinatarios de la presente Lineamiento.
k. Registrar, modificar o revocar la inscripción de los bancos de datos personales en la Dirección Nacional de Protección de Datos Personales del Ministerio de Justicia.
l. Informar a la Dirección Nacional de Protección de Datos Personales y/o titulares de datos personales cuando se presenten violaciones a las medidas de seguridad sobre los datos.

II. **Responsable del Tratamiento**
Personal designado por la ONP para realizar el tratamiento de los datos personales. Puede ser ejecutado por un órgano interno o mediante servicios brindados por contratistas (encargado), cumpliendo lo siguiente:

a. No realizar el tratamiento de datos para una finalidad diferente a la definida por el titular del banco de datos personales.

V° B° JENNIFER AYLLÓN BULNES ONP

V° B° PABLO BOLAÑOS ONP

b. Realizar oportunamente la actualización, rectificación o supresión de los datos.
c. Conservar los datos personales bajo las condiciones de seguridad dispuestas en la presente directiva para preservar su confidencialidad, integridad y disponibilidad.
d. Informar oportunamente al titular del banco de datos personales, a través del Gestor de Seguridad de la Información, sobre los incidentes de seguridad presentados en el tratamiento de los datos, implementando mecanismos que permitan identificar el detalle del evento suscitado.

e. **Medidas de seguridad para la protección de datos personales**

Producto de los lineamientos definidos en el presente documento, la ONP adoptará una serie de medidas de seguridad orientadas a proteger la información bajo su responsabilidad, incluyendo por consiguiente, los datos personales. Sin embargo, es oportuno precisar las siguientes medidas específicas que deben aplicarse inequívocamente sobre el tratamiento de los datos, encontrándose alineadas con lo dispuesto en los apartados anteriores:

i. Para los sistemas informáticos que manejen bancos de datos personales:

   a. Gestión de accesos y privilegios, respetando los lineamientos detallados en el numeral 8.3 Lineamientos de Control de Acceso incluidos en el presente documento.
   b. Control de registros que provean evidencia sobre las interacciones con los datos.

ii. Los ambientes y espacios físicos donde se procese, almacene o transmita datos personales deben operar bajo estrictas medidas de seguridad que permitan evitar potenciales daños a las instalaciones y prevenir accesos no autorizados.
iii. La OTI efectuará copias de respaldo de los bancos de datos personales, además deben implementarse procedimientos de restauración que permitan garantizar la integridad de los datos y su disponibilidad oportuna.
iv. La transferencia lógica o electrónica de los datos personales hacia ambientes externos a la ONP, se realizará bajo las condiciones de seguridad necesarias para garantizar su confidencialidad, integridad y disponibilidad.
v. El traslado de información que contenga datos personales será efectuado adoptando las medidas pertinentes para impedir el acceso o manipulación de personal no autorizado.
vi. La eliminación de los medios que contengan datos personales se realizará bajo medidas estrictas de seguridad, de forma que se evite el acceso a la información contenida en los mismos o su recuperación posterior. La acción descrita deberá ser efectuada por el encargado del tratamiento de la información en coordinación con el Gestor de Seguridad de Información.

8.12.5. Protección de los registros de la ONP y controles criptográficos

a. Los registros de la organización se deberán almacenar de forma segura, teniendo en cuenta la clasificación de la información (registros contables, registros de bases de datos, registros de auditoría, etc.), y sus niveles de confidencialidad (público, restringido y confidencial).
b. El Gestor de Seguridad de la Información, en coordinación con los responsables de los órganos y propietarios de la información, definirá los controles de protección para los registros importantes de la ONP, así como los procedimientos para su tratamiento y eliminación.
c. La información de la ONP deberá protegerse por un periodo de 10 años, mientras que el resto de los registros deben protegerse por lo menos 5 años, según el Decreto Ley Nº 19414, Ley de Defensa, Conservación e Incremento del Patrimonio Documental de la Nación.
d. Se deberá implantar los controles y medidas apropiadas para evitar la pérdida, destrucción o falsificación de los registros y la información esencial de la Institución.
e. La OTI deberá analizar y evaluar la inclusión de un estándar de uso de controles criptográficos en las aplicaciones para la entidad. Este estándar debe contener el detalle respecto al algoritmo, tamaño, gestión de las llaves, el soporte de las técnicas de encriptación y el alcance del mismo según el tipo de aplicación.
f. La OTI definirá la gestión de las llaves de encriptación incluyendo la protección contra modificación, pérdida y destrucción. Las llaves secretas o privadas o llaves maestras que se generen deberán estar bajo la custodia de la OTI.
g. El contenido de los acuerdos de nivel de servicio o de los contratos con terceros de servicios criptográficos (por ejemplo una autoridad certificadora) debería cubrir los aspectos de las obligaciones, fiabilidad de los servicios y tiempos de respuesta para su suministro.

8.12.6. Revisiones de la seguridad de la información

a. Las revisiones independientes de la seguridad de la información serán realizadas en la ONP, los cuales deben de realizarse una vez al año y será ejecutado por un tercero. Los responsables del seguimiento de dichas acciones serán el Gestor de la Seguridad de la Información y del encargado en el órgano o equipo de trabajo responsable del proceso.
b. La OTI en su plan de revisiones deberá evaluar el cumplimiento de los lineamientos y normativas de seguridad, al menos una vez al año la efectividad de los lineamientos de seguridad de la información y deberá impulsar los cambios correspondientes de ser necesarios, lo que será ejecutado por el Gestor de la Seguridad de la Información o quien éste designe, y el resultado obtenido de las revisiones será evidenciado en un informe dirigido a Jefatura OTI. El seguimiento de este cumplimiento será efectuado por el encargado del órgano o equipo de trabajo en el alcance de la revisión y por el Gestor de Seguridad de la Información.
c. Dentro del plan de revisiones de la OTI, se efectuará la revisión de cumplimiento técnico por lo menos una vez al año. Dicho seguimiento estará a cargo de la OTI y la supervisión del servicio en el alcance de la revisión.
d. Es responsabilidad del supervisor de los servicios velar por su cumplimiento e implementación

9. CAMBIOS A LA VERSION ANTERIOR

a. De acuerdo a lo señalado por el Órgano de Control Institucional, en el párrafo b) del numeral 8.12.6, se ha precisado la entrega de un informe de las revisiones de cumplimiento de los lineamientos y normativas de seguridad de información.
b. Se ha modificado el literal d) del numeral 8.2.6 y el literal c) del numeral 8.11.4 en base a las recomendaciones de la Oficina de Gestión de Riesgos.
c. Se actualizó la codificación de los formatos.

10. DISPOSICION FINAL

Dejar sin efecto la directiva "Lineamientos de Seguridad de la Información" (DIR-OTI-02/02)

11. FORMATOS

DIR-02/01-A Compromiso de Confidencialidad

ONP Oficina de Normalización Previsional	COMPROMISO DE CONFIDENCIALIDAD	Versión: 1.0
INTERNO	FORMATO	Fecha de formato:

COMPROMISO DE CONFIDENCIALIDAD

Yo, _____, identificado con DNI N°_____, Trabajador de la Institución_ _____Con R.U.C. _____, Encargado de efectuar labores de _____ _____, en el marco del contrato de servicio Nº _____ ., me comprometo a no difundir a terceros información de la ONP, a la que pueda tener acceso durante el periodo del servicio. En caso de incumplimiento de lo indicado, la institución se reserva el derecho de iniciar las acciones legales correspondientes.

Asimismo, me comprometo a no revelar información oral, escrita, secretos industriales relacionados con los productos, servicios, políticas o prácticas de negocio, políticas de la seguridad de la información de la ONP u otros. En caso que incumpliera con cuales quiera de las obligaciones estipuladas en esta cláusula, la Oficina de Normalización Provisional estará en potestad de iniciar todas las acciones judiciales o extrajudiciales necesarias para resarcirse del perjuicio. Esta obligación se hace extensiva inclusive hasta los dos años después del retiro del trabajador de la empresa contratada.

Lima, _de _____ del 201__.

_____
FIRMA (igual a DNI)
Nombre completo
DNI:

DIR-02/01-B Cumplimiento de Politicas de Seguridad de Información

ONP	DECLARACION JURADA – CUMPLIMIENTO DE POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
INTERNO	FORMATO	Fecha de formato:

DECLARACION JURADA

Yo, _____, identificado con DNI N°_____, que a la fecha desempeño el cargo de _____, en el marco de del contrato Nro. _____., **DECLARO** lo siguiente:

Primero:

- Haber comprendido la Directiva "Lineamientos de Seguridad de la Información" (DIR-02/01).

Segundo:

- Cumplir con las cláusulas que apliquen de la Directiva indicada en el primer punto.

Tercero:

- En caso incumpliera alguna de las cláusulas de la Directiva de la indicada en el primer punto, la institución se reserva el derecho de iniciar las acciones legales correspondientes en caso apliquen.

Lima, ___ de _____ del 201__.

_____
FIRMA (igual a DNI)
Nombre completo
DNI:

Anexo N° 11 – Reporte Final de Mensajería.

En vista vertical, pero deberá ser presentado en forma horizontal las 2 imágenes integradas en un mismo reporte de Excel.

FORMATO DE REPORTE FINAL DE MENSAJERIA

OFICINA DE ONP

PERIODO :

ITEM	SEDE	MES	TIPO DE ENVIO	FECHA DE ORDEN (RECEPCION)	N° DE GUIA	CORRELATIVO DE GUIA	AREA USUARIA	TIPO DE DOCUMENTO	NUMERO DE DOCUMENTO	DESTINATARIO	DIRECCIÓN	DEPARTAMENTO	PROVINCIA	DISTRITO
												LIMA		
												LIMA		
												LIMA		

Sede: Centro de Atención a nivel Nacional
Tipo de Envio: Local
Tipo de Documento: Carta, Memo, Oficio,
Plazo de Entrega: Establecido en las Bases
Plazo de Devolución: Establecido en las Bases
Bajo Puerta: Solo llenar el campo con la palabra "SI", siempre y cuando el cargo haya sido entregado bajo puerta
Estado: Entregado, Devuelto, Pendiente, Motivo (Denuncia Policial)
Detalle de Estado: En los casos que sea una correspondencia devuelta, describir el motivo por la cual fue devuelta la correspondencia
Estado de Pago: Pagado o Pendiente

+

CORRESPONDENCIA								DENUNCIA POLICIAL POR PERDIDA O ROBO						
FECHA DE RECOJO DE LA CORRESPONDENCIA	PLAZO DE ENTREGA	FECHA 1ERA VISITA	FECHA DE ENTREGA AL DESTINATARIO	PLAZO DE DEVOLUCION	FECHA DE DEVOLUCION DEL DOCUMENTO CARGO (*)	GUIA DEVOLUCION	BAJA PUERTA?	FECHA DE PRODUCIDO EL HECHO	FECHA DE REGISTRO DE LA DENUNCIA	COMISARIA DONDE SE REGISTRO LA DENUNCIA	ESTADO	DETALLE ESTADO	PRECIO UNITARIO DEL SERVICIO	ESTADO DE PAGO

Anexo N° 12 – Reporte Final de denuncias policiales por pérdida o robo.

REPORTE FINAL DE DENUNCIAS POLICIALES POR PÉRDIDA O ROBO

Nº	Tipo de documento extraviado o robado	Código o número del documento	Numero de guía	Correlativo del documento	Nombre del destinatario	Dirección del destinatario	Estado de documento

Leyenda:
Estado de Documento: Cargo o Correspondencia

II. REQUISITOS DE CALIFICACIÓN

A	**CAPACIDAD LEGAL**
	HABILITACIÓN
	Requisitos: El postor debe contar con la concesión postal vigente en el ámbito de operación requerido (local y regional) aprobado por el Ministerio de Transportes y Comunicaciones. **Importante** *De conformidad con la Opinión N° 186-2016/DTN, la habilitación de un postor, está relacionada con cierta atribución con la cual debe contar el proveedor para poder llevar a cabo la actividad materia de contratación, este es el caso de las actividades reguladas por normas en las cuales se establecen determinados requisitos que las empresas deben cumplir a efectos de estar habilitadas para la ejecución de determinado servicio o estar autorizadas para la comercialización de ciertos bienes en el mercado.* Acreditación: Copia del contrato de concesión para la prestación del servicio postal y de la Resolución Directoral que aprueba la concesión postal expedida por la Dirección General de Concesiones en Comunicaciones del Ministerio de Transportes y Comunicaciones o entidad competente. **Importante** *En el caso de consorcios, cada integrante del consorcio que se hubiera comprometido a ejecutar las obligaciones vinculadas directamente al objeto de la convocatoria debe acreditar este requisito.*

B	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.1	**INFRAESTRUCTURA ESTRATÉGICA**
	Requisitos: Contar con por lo menos un (1) local en la ciudad de Lima y/o de la Provincia Constitucional del Callao para el desarrollo integral de sus operaciones. Acreditación: Copia de documentos que sustenten la propiedad, la posesión, el compromiso de compra venta o alquiler u otro documento que acredite la disponibilidad de la infraestructura estratégica requerido. **Importante** *En el caso que el postor sea un consorcio los documentos de acreditación de este requisito pueden estar a nombre del consorcio o de uno de sus integrantes.*
B.2	**CALIFICACIONES DEL PERSONAL CLAVE**
B.2.1	**FORMACIÓN ACADÉMICA**
	Requisitos:

	Bachiller universitario o Título profesional técnico en Administración, Contabilidad, Economía, Derecho, Estadística,Investigación Operativa o Ingeniería del personal, del personal requerido como "Supervisor". Acreditación: El Bachiller universitario o título profesional técnico será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ // o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link : http://www.titulosinstitutos.pe/, según corresponda. En caso el bachiller universitario o título profesional técnico no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.
B.2.2	**CAPACITACIÓN**
	Requisitos: 16 horas lectivas en la Ley de Procedimiento Administrativo General – Ley N° 27444, del personal clave requerido como "Supervisor". Acreditación: Se acreditará con copia simple de constancias o certificados. **Importante** *Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.*
B.3	**EXPERIENCIA DEL PERSONAL CLAVE**
	Requisitos: Cuatro (4) años como mínimo como supervisor o coordinador o jefe en mensajería y/o Courier y/o servicio postal o de Operaciones de mensajería, del personal requerido como "Supervisor". De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado. Acreditación: La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto. **Importante** • *Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.* • *En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.* • *Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.* • *Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con*

	aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.
C	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/ 1, 000 000.00 (Un millón 00/100 soles) por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Se consideran servicios similares a los siguientes: • Servicios de mensajería local y/o • Servicio postal y/o • Courier local y/o • Encomienda y/o • Paquetería o carga y/o • Servicios de Notificación de documentos a nivel local. Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago[1], correspondientes a un máximo de veinte (20) contrataciones. En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo indicado en las bases** referido a la Experiencia del Postor en la Especialidad. En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados. En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato. Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales. Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en

[1] Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

> *"… el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"*
> *(…)*
> *"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".*

	caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo indicado en las bases.** Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda. Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo indicado en las bases** referido a la Experiencia del Postor en la Especialidad. **Importante** • *Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.* • *En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*