Resolución Directoral Ejecutiva

Nro. 179-2020-MINEDU/VMGI-PRONABEC

Lima, 10 de noviembre de 2020

VISTOS:

El Informe N° 174-2020-MINEDU/VMGI-PRONABEC-OITEC de la Oficina de Innovación Tecnología, el Informe N° 039-2020-MINEDU/VMGI-PRONABEC-OPP-UDGP, ratificado con l Informe 052-2020-MINEDU/VMGI-PRONABEC-OPP-UDGP de la Oficina de Planificación y 'resupuesto, el Informe N° 194-2020-MINEDU/VMGI-PRONABEC-OAJ y el el Oficio N° 441-2020-MINEDU/VMGI-PRONABEC-OAJ de la Oficina de Asesoría Jurídica, y demás recaudos que se acompañan al Expediente N° 34149-2020 y 49169-2020 (SIGEDO); y,

CONSIDERANDO:

Que, el artículo 4 de la Ley N° 27658, Ley Marco de Modernización del Estado Peruano, señala que la finalidad fundamental del proceso de modernización de la gestión del Estado es la *"(…) obtención de mayores niveles de eficiencia del aparato estatal, de manera que se logre una mayor atención de la ciudadanía, priorizando y optimizando el uso de los recursos públicos (…)"*;

Que, mediante el Decreto Supremo N° 066-2011-PCM, se aprobó el "*Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0*". Asimismo; y, por Decreto Legislativo N° 1412, se aprobó la Ley de Gobierno Digital;

Que, mediante la Resolución Directoral Ejecutiva N° 535-2015-MINEDU-VMGI-PRONABEC, del 20 de noviembre de 2015, se aprobó la Norma Técnica denominada *"Lineamientos de Política de seguridad de la Información del Programa Nacional de Becas y Crédito Educativos";*

Que, la Resolución Ministerial N° 004-2016-PCM, aprueba el uso obligatorio de la Norma Técnica Peruana *"NTP ISO/IEC 270001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da Edición"*, en todas las entidades integrantes del Sistema Nacional de Informática;

Que, mediante la Resolución Directoral Ejecutiva N° 112-2016-MINEDU-VMGI-PRONABEC, del 23 de febrero de 2016, se aprobó la *"Política de Seguridad de la Información del Programa Nacional de Becas y Crédito Educativo";*

Que, mediante la Resolución Directoral Ejecutiva N° 310-2016-MINEDU-VMGI-PRONABEC, del 20 de mayo del 2016, se aprobó el documento de naturaleza técnica denominado *"Documentos de Soporte de Gestión de la Seguridad de la Información (SGSI) del Programa Nacional de Becas y Crédito Educativo";*

Que, mediante la Resolución Directoral Ejecutiva N° 410-2016-MINEDU-VMGI-PRONABEC, del 28 de junio de 2016, se aprobó el documento de naturaleza técnica denominado *"Documentos de Soporte al Sistema de Gestión de la Seguridad de la Información – SGSI basados en los lineamientos de la Norma Técnica "NTP ISO/IEC 27001:2014 del PRONABEC"*;

Que, mediante la Resolución Ministerial N° 705-2017-MINEDU se aprobó el Manual de Operaciones del PRONABEC, cuyo artículo 27 señala que la Oficina de Innovación y Tecnología tiene entre sus funciones diseñar, elaborar y proponer la normativa necesaria para la operatividad del Gobierno Electrónico en el PRONABEC, en cumplimiento de las políticas nacionales; así como, implementar y supervisar el Sistema de Gestión de Seguridad de la Información en el PRONABEC, en cumplimiento de la normativa vigente;

Que, mediante el Decreto de Urgencia N° 007-2020, se aprobó el Marco de Confianza Digital con el objeto de establecer las medidas necesarias para garantizar la confianza de las personas en su interacción con los servicios digitales prestados por entidades públicas y organizaciones del sector privado en el territorio nacional;

Que, mediante el Informe N° 174-2020-MINEDU/VMGI-PRONABEC-OITEC, la Oficina de Innovación y Tecnología señala que la *"Política de Seguridad de la Información del Programa Nacional de Becas y Crédito Educativo (PRONABEC)"*, aprobada con Resolución Directoral Ejecutiva N° 112-2016-MINEDU-VMGI-PRONABEC, adolece de actualizaciones de responsabilidades, políticas y objetivos de seguridad de la información que se alineen con el plan estratégico institucional, con la Política Nacional de Gobierno Electrónico y nuevos marcos normativos de cumplimiento para el sector público, que refuerzan y precisan la importancia de contar con instrumentos que aseguren la gestión de la seguridad de la información;

Que, en ese contexto, la precitada Oficina elaboró la propuesta de Directiva *"Disposiciones de Seguridad de la Información del PRONABEC"* con el objetivo de establecer las medidas que regulen la gobernanza de la seguridad de la información y el resguardo de los activos de la información, recursos informáticos o plataformas tecnológicas donde se procesa y almacena información en el PRONABEC frente a amenazas, internas o externas, deliberadas o accidentales con el fin de mitigar los riesgos. Así, establece disposiciones específicas sobre la organización de la seguridad de la información, seguridad relativa a los recursos humanos, activos de la información, control de accesos, criptografía, instalaciones y entorno físico, operaciones, comunicaciones, adquisición, desarrollo y mantenimiento de sistemas, entre otros, así como las responsabilidades;

Que, asimismo, la mencionada Oficina señala que la aprobación de la propuesta normativa antes mencionada conlleva la derogación de la normativa referida a las Políticas de Seguridad de la Información del PRONABEC aprobadas previamente mediante las Resoluciones Directorales Ejecutivas N° 535-2015-MINEDU-VMGI-PRONABEC, N° 112-2016-MINEDU-VMGI-PRONABEC, N° 310-2016-MINEDU-VMGI-PRONABEC y N° 410-2016-MINEDU-VMGI-PRONABEC, dado que, la nueva directiva consolida en un solo documento la regulación y procedimientos sobre seguridad de la información;

Que, de otro lado, la Oficina de Innovación y Tecnología manifiesta que la precitada propuesta de Directiva cuenta con la conformidad del Comité de Gobierno Digital del PRONABEC, según el Acta de Reunión N° 005-2020/PRONABEC-CGD de fecha 15 de junio de 2020;

Que, de igual manera, la referida Oficina precisa que con la propuesta de Directiva *"Disposiciones de Seguridad de la Información del PRONABEC"* se da cumplimiento a la Recomendación N° 7 de la Carta de Control Interno PRONABEC – Auditoría Taboada & Asociados S.C. Periodo 2016, referida a la revisión, actualización y formalización de todas las políticas y procedimientos relacionados a la Seguridad de la Información del PRONABEC;

Que, mediante el Informe N° 039-2020-MINEDU/VMGI-PRONABEC-OPP-UDGP, ratificado mediante el Informe 052-2020-MINEDU/VMGI-PRONABEC-OPP-UDGP, la Unidad de

Desarrollo y Gestión de Procesos de la Oficina de Planificación y Presupuesto, con la conformidad de esta última, indica que ha verificado que, en el marco de sus competencias, la Oficina de Administración y Finanzas, la Oficina de Atención al Ciudadano y Gestión Documentaria y la Oficina de Gestión del Talento a través del Memorándum Nº 1670-2020-MINEDU/VMGI-PRONABEC-OAF, Memorándum Nº 143-2020-MINEDU/VMGI-PRONABEC-OAGD e Informe Nº 357-2020-MINEDU/VMGI-PRONABEC-OGTA, respectivamente, emitieron opinión técnica favorable respecto de la propuesta normativa elaborada por la Oficina de Innovación y Tecnología. Asimismo, señala que la propuesta normativa guarda relación causal y aplicación coherente con lo establecido en la Ley N° 29837, su Reglamento, el Manual de Operaciones del PRONABEC y la Norma Técnica Peruana "NTP-ISO/IEC 2700:2014"; y, en consecuencia, otorga opinión técnica favorable en materia de instrumento de gestión administrativa;

Que, a través del Oficio N° 00193-2020-MINEDU/SPE-OPEP-UNOME, la Unidad de Organización y Métodos de la Oficina de Planificación Estratégica y Presupuesto del Ministerio de Educación, ha precisado el Oficio Múltiple N° 00004-2020-MINEDU/SPE-OPEP-UNOME, indicando que la aprobación de documentos cuyo ámbito de aplicación se establezcan al interior de estas dependencias (funcionamiento interno), corresponde a la oficina de planificación u organización, o la que haga sus veces en la dependencia, a fin de establecer la ruta interna de formulación, validación y aprobación de los documentos, así como registrar y codificar los mismos;

Que, mediante el Informe N° 194-2020-MINEDU/VMGI-PRONABEC-OAJ, la Oficina de Asesoría Jurídica, señala que la Oficina de Innovación y Tecnología tiene como una de sus funciones diseñar, elaborar y proponer la normativa necesaria para la operatividad del Gobierno Electrónico en el PRONABEC, por lo que, al amparo de ello ha propuesto la aprobación de la Directiva "Disposiciones de Seguridad de la Información del PRONABEC"; cuya estructura comprende el Objetivo, Finalidad, Alcance, Base Normativa, Glosario de Términos, Disposiciones Generales y Específicas y Responsabilidades de las áreas intervinientes;

Que, del mismo modo, la referida Oficina verifica que la propuesta de Directiva *"Disposiciones de Seguridad de la Información del PRONABEC"*, formulada por la Oficina de Innovación y Tecnología, no contraviene lo dispuesto por la Ley N° 29837, su Reglamento y el Manual de Operaciones del PRONABEC y cuenta con la opinión técnica favorable de la Oficina de Gestión de Talento, la Oficina de Atención al Ciudadano y Gestión Documentaria, la Oficina de Administración y Finanzas y la Oficina de Planificación y Presupuesto;

Que, por su parte, con el Oficio N° 441-2020-MINEDU/VMGI-PRONABEC-OAJ, el mencionado órgano de asesoramiento señala que, de acuerdo con lo indicado por la referida Unidad de Organización y Métodos, habiéndosele asignado a la propuesta la codificación correspondiente por parte de la Oficina de Planificación y Presupuesto, corresponde continuar con la tramitación de la propuesta normativa antes mencionada;

Que, asimismo señala que, en la medida que la directiva antes mencionada consolida la regulación y procedimiento referidos a la seguridad de la información, corresponde la derogación de la Resolución Directoral Ejecutiva N° 535-2015-MINEDU-VMGI-PRONABEC, que aprobó la Norma Técnica denominada *"Lineamientos de Política de seguridad de la Información del Programa Nacional de Becas y Crédito Educativo"*, la Resolución Directoral Ejecutiva N° 112-2016-MINEDU-VMGI-PRONABEC, que aprobó la *"Política de Seguridad de la Información del Programa Nacional de Becas y Crédito Educativo"*, la Resolución Directoral Ejecutiva N° 310-2016-MINEDU-VMGI-PRONABEC, que aprobó el documento de naturaleza técnica denominado *"Documentos de Soporte de Gestión de la Seguridad de la Información (SGSI) del Programa Nacional de Becas y Crédito Educativo"* y la Resolución Directoral Ejecutiva N° 410-2016-MINEDU-VMGI-PRONABEC, que aprobó los documentos de naturaleza técnica denominada *"Documentos de Soporte al Sistema de Gestión de la Seguridad de la Información – SGSI basados en los lineamientos de la Norma Técnica "NTP ISO/IEC 27001:2014 del PRONABEC"*; la misma que no contraviene el marco normativo vigente, por lo que resulta legalmente viable;

Que, conforme lo establecen los artículos 10 y 11 del Manual de Operaciones del PRONABEC, aprobado por la Resolución Ministerial N° 705-2017-MINEDU, la Dirección Ejecutiva es la máxima autoridad administrativa y tiene entre sus funciones, la de dirigir, organizar y supervisar la gestión del PRONABEC, así como expedir actos resolutivos en materia de su competencia, en el marco de la normativa aplicable; y,

Con el visto de la Oficina de Innovación y Tecnología, de la Oficina de Administración y Finanzas, de la Oficina de Atención al Ciudadano y Gestión Documentaria, de la Oficina de Gestión del Talento, de la Oficina de Planificación y Presupuesto, y de la Oficina de Asesoría Jurídica; y de conformidad con lo establecido en la Ley N° 29837, Ley que crea el Programa Nacional de Becas y Crédito Educativo - PRONABEC, modificada por la Sexta Disposición Complementaria Modificatoria de la Ley N° 30281, Ley del Presupuesto del Sector Público para el Año Fiscal 2015; su Reglamento, aprobado por el Decreto Supremo N° 013-2012-ED y modificatorias; y el Manual de Operaciones del PRONABEC, aprobado mediante la Resolución Ministerial N° 705-2017-MINEDU;

SE RESUELVE:

Artículo 1.- Aprobar la Directiva denominada *"Disposiciones de Seguridad de la Información del PRONABEC"*, conforme al anexo que forma parte integrante de la presente resolución.

Artículo 2.- Derogar la Resolución Directoral Ejecutiva N° 535-2015-MINEDU-VMGI-PRONABEC, que aprobó la Norma Técnica denominada *"Lineamientos de Política de seguridad de la Información del Programa Nacional de Becas y Crédito Educativo"*; la Resolución Directoral Ejecutiva N° 112-2016-MINEDU-VMGI-PRONABEC, que aprobó la *"Política de Seguridad de la Información del Programa Nacional de Becas y Crédito Educativo"*; la Resolución Directoral Ejecutiva N° 310-2016-MINEDU-VMGI-PRONABEC, que aprobó el documento de naturaleza técnica denominado *"Documentos de Soporte de Gestión de la Seguridad de la Información (SGSI) del Programa Nacional de Becas y Crédito Educativo*"; y, la Resolución Directoral Ejecutiva N° 410-2016-MINEDU-VMGI-PRONABEC, que aprobó los documentos de naturaleza técnica denominada *"Documentos de Soporte al Sistema de Gestión de la Seguridad de la Información – SGSI basados en los lineamientos de la Norma Técnica "NTP ISO/IEC 27001:2014 del PRONABEC"*.

Artículo 3.- Notificar la presente resolución a los órganos de Línea, de Apoyo, de Asesoramiento y Órganos Desconcentrados del PRONABEC

Articulo 4.- Publicar la presente resolución en el portal electrónico institucional del PRONABEC.

Regístrese, comuníquese y publíquese.

Firmado Digitalmente por: MESINAS MONTERO Jorge Manuel FAU 20546798152 hard
Razón: DIRECTOR EJECUTIVO
Ubicación: PRONABEC
Fecha: 10/11/2020 20:45:02

JORGE MESINAS MONTERO
Director Ejecutivo
Programa Nacional de Becas y Crédito Educativo

Directiva

“DISPOSICIONES DE SEGURIDAD DE LA INFORMACIÓN DEL PRONABEC”

Resolución de Aprobación			
Resolución Directoral Ejecutiva N° 179-2020-MINEDU/VMGI-PRONABEC			
Código	Versión	Páginas	Fecha de aprobación
DI-001-01-MINEDU/PRONABEC	1.0	31	10 de noviembre de 2020

Control de Cambios		
Versión	**Sección / Ítem**	**Descripción del cambio:**
1.0	----	Nuevo

1. OBJETIVO

Establecer las disposiciones que regulen la gobernanza de la seguridad de la información y el resguardo de los activos de información, recursos informáticos o plataformas tecnológicas donde se procesa y almacena información en el PRONABEC frente a amenazas, internas o externas, deliberadas o accidentales con el fin de mitigar los riesgos.

2. FINALIDAD

Gestionar adecuadamente la seguridad de la información que permita asegurar la confidencialidad, integridad y disponibilidad de la información institucional la cual forma parte integrante de los procesos que permiten fortalecer el acceso a una formación de calidad con equidad en los estudiantes de la educación técnico-productiva y superior a través del PRONABEC, en aras de cumplir con el OEI 02 y AEI 02.09 del Plan Estratégico Institucional – PEI del MINEDU 2019 – 2022, aprobado por la Resolución Ministerial N° 737-2018-MINEDU; así como también:

a) Establecer, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información mediante la implementación de controles que permitan hacer frente a amenazas de ataque o intromisión, error, actos de la naturaleza (inundación, incendio, etc.) o vulnerabilidades inherentes a su uso, en cumplimiento de la Norma Técnica Peruana ISO/IEC 27001:2014 “Tecnología de la Información. Técnicas de Seguridad. Sistemas de Seguridad de la Información”.

b) Garantizar el adecuado tratamiento de activos de información que incluya datos personales conforme a lo establecido en la Ley de Protección de Datos Personales, su Reglamento y demás normas relacionadas.

c) Promover y concientizar a los usuarios respecto a las responsabilidades por el uso de la información, así como del cumplimiento de las medidas y controles de Seguridad de la Información.

d) Cumplir con las normas legales y reglamentos estipulados por la ley y los organismos reguladores correspondientes, referidas a la seguridad de la información y protección de datos personales.

3. ALCANCE

Las disposiciones establecidas en la presente directiva son de observancia obligatoria para todo el personal bajo los distintos regímenes laborales del Programa Nacional de Becas y Crédito Educativo (PRONABEC).

Asimismo, es aplicable a las personas bajo contratos de locación y proveedores que prestan servicios al PRONABEC cuyas obligaciones deberán estar consignadas en los acuerdos de confidencialidad que suscriban.

Comprende toda la información desarrollada, gestionada, transmitida, almacenada y de autoría propia del PRONABEC, así como también, a todos los sistemas de información asociados con el almacenamiento, procesamiento y trasmisión de información generada por y a favor del PRONABEC.

4. BASE NORMATIVA

- Ley N° 27269: Ley de Firmas y Certificados Digitales y modificatorias.
- Ley N° 27291: Ley que modifica el código civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica.
- Ley N° 27658: Ley Marco de Modernización de la Gestión del Estado y modificatorias.
- Ley N° 27806: Ley de Transparencia y Acceso a la Información Pública y modificatorias.
- Ley N° 28493: Ley que regula el uso del Correo Electrónico comercial no solicitado (SPAM) y modificatoria.
- Ley N° 28530: Ley de Promoción de Acceso a Internet para personas con discapacidad y adecuación del espacio físico en cabinas públicas de internet y modificatorias.
- Ley N° 29733: Ley de Protección de Datos Personales y modificatorias.
- Ley N° 30096: Ley de Delitos Informáticos y modificatorias.
- Decreto Legislativo N° 822: Ley de Derechos de Autor y modificatorias.
- Decreto Legislativo N° 1353, que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses y modificatorias.
- Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital y modificatorias.
- Decreto Supremo N° 066-2011-PCM, que aprueba el “Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0”.
- Decreto Supremo N° 003-2013-JUS, que aprueba el reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales y modificatorias.
- Decreto Supremo N° 010-2019-RE, que ratifica el “Convenio sobre la Ciberdelincuencia”.
- Decreto de Urgencia N° 007-2020, que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática y modificatoria.
- Resolución Ministerial N° 705-2017-MINEDU, que aprueba el Manual de Operaciones (MOP) del Programa Nacional de Becas y Crédito Educativo (PRONABEC).
- Resolución Ministerial N° 087-2019-PCM, que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
- Resolución de Secretaría General N° 041-2019-MINEDU, que aprueba los procedimientos para la elaboración de procedimientos, instructivos y formatos institucionales del MINEDU.
- Resolución de Secretaria General N° 073-2019-MINEDU, que aprueba la Directiva N° 005-2019-MINEDU/SPE-OPEP-UNOME, que establece el marco normativo para la elaboración aprobación y derogación de actos resolutivos, así como elaboración y modificación de documentos de gestión, normativos y orientadores del Ministerio de Educación.
- Resolución de Secretaría General N° 090-2020-MINEDU, que suspende la aplicación de la Directiva N° 005-2019-MINEDU/SPE-OPEP-UNOME.
- Resolución Directoral N° 019-2013-JUS/DGPDP, que aprueba la Directiva de Seguridad de la información administrada por lo Bancos de Datos Personales.

5. GLOSARIO DE TÉRMINOS

a) **Activo de información:** Cualquier información que tiene valor para la Entidad y para el Sistema de Gestión de Seguridad de la Información. Se consideran también los recursos humanos, tecnológicos que intervienen en el tratamiento directo o indirecto de la información, así como sus procesos y actividades.

b) **Amenaza:** Cualquier factor que tiene el potencial para explotar una debilidad y dar lugar a algún tipo de daño a la información o a la institución.

c) **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarlas de manera objetiva, para determinar el grado de cumplimiento de criterios pre-establecidos.

d) **Buzón compartido:** Es un buzón de correo electrónico virtual para permitir la recepción y envío de mensajes de correo desde una o más cuentas de correo de manera compartida, además permite compartir un calendario común. Un buzón compartido también puede servir como una cuenta de correo genérica.

e) **Clasificación de la Información:** Acción de identificar y clasificar los activos de información en términos de la sensibilidad e importancia para la Entidad.

f) **Confidencialidad:** Propiedad de la información que hace que no esté disponible o que sea revelada a individuos o entidades no autorizados.

g) **Control:** Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la entidad que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

h) **Control de acceso:** Medios o mecanismo para garantizar que el acceso a los activos de manera autorizada y restringida, basado en los requerimientos de negocios y los requisitos de seguridad.

i) **Comité de Gobierno Digital:** El Comité de Gobierno Digital (CGD) fue establecido con Resolución Directoral Ejecutiva N° 263-2019-MINEDU-VMGI-PRONABEC y es responsable de gestionar, mantener y documentar el Modelo de Gestión Documental (MGD), Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de la Seguridad de la Información (SGSI) del PRONABEC.

j) **Credencial de acceso:** Corresponde al mecanismo mediante el cual se le asigna una identificación única e irrepetible a una persona, para que tenga acceso a las aplicaciones de la Entidad, con el propósito de desempeñar las tareas encomendadas.

k) **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.

l) **Disponibilidad:** Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada.

m) **Dispositivo móvil:** Aparato de tamaño portable que tiene capacidad de acceso, almacenamiento y/o procesamiento de información, disponiendo además de conexión permanente o intermitente a una red de comunicaciones tales como la Notebook, Tablet o Smartphone.

n) **Equipo informático:** Dispositivo electrónico que permite procesar información y datos con programas diseñados para ello, incluye a las computadoras, impresoras, escáneres y los dispositivos móviles.

o) **Evento:** Un suceso que puede ser interno o externo a la Entidad, que ocurren en un momento determinado y son originados por una causa especifica.

p) **Grupo de colaboración:** Un grupo colaborativo es un espacio de trabajo de colaboración para mensajes de grupo, intercambio de archivos y calendario grupal integrado con los servicios de correo electrónico asignado al personal del PRONABEC.

q) **Incidente de seguridad de la información:** Evento no deseado que genera amenaza a la seguridad de la información y que tiene una probabilidad significativa de comprometer a la operatividad de la Entidad.

r) **Información:** Cualquier forma de registro de contenidos susceptibles a ser procesados, distribuidos y almacenados, pudiendo estar en formato electrónico, óptico, magnéticos u otro medio de almacenamiento.

s) **Integridad:** Propiedad de precisión y completitud de la información.

t) **Jefe inmediato:** Para efectos de la presente Directiva se considera como jefe inmediato al responsable de la dirección del órgano o unidad orgánica conforme a la estructura orgánica establecida en el Reglamento de Organización y Funciones del PRONABEC vigente.

u) **Lista de distribución:** Es un servicio para distribuir mensajes de correo electrónico a dos o más personas al mismo tiempo permitiendo difundir comunicados masivos a sus miembros.

v) **Medios removibles:** Dispositivos de almacenamiento de información extraíbles de un equipo informático tales como cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

w) **Oficial de Seguridad de la Información:** El Oficial de Seguridad de la Información es el responsable del Sistema de Gestión de la Seguridad de la Información (SGSI) y reporta al Comité de Gobierno Digital (CGD). El rol está designado con Resolución Directoral Ejecutiva N° 263-2019-MINEDU-VMGI-PRONABEC.

x) **Personal del PRONABEC:** Comprende a los servidores civiles designados o asignados bajo Contratación Administrativa de Servicios; así como a aquellas personas contratadas en el marco de la Ley N° 29806, Ley que regula la contratación de personal altamente calificado en el Sector Público.

y) **Propietario de activo:** Es el funcionario o servidor asignado de garantizar que el activo asignado bajo su responsabilidad esté protegido con los controles definidos en el SGSI y que le apliquen a dicho activo; es el responsable por la afectación de la confidencialidad, integridad y disponibilidad del mismo, en cualquiera de los procesos que se encuentre involucrado.

z) **Redes sociales:** Corresponde a los portales de redes sociales públicos como Facebook, Instagram, Twitter, etc.).

aa) **Riesgo:** Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen institucional, etc.) y se pueden aplicar a niveles diferentes (operativo, estratégico, organización).

bb) **Seguridad de la información:** Todas las acciones orientadas a preservar la integridad, confidencialidad y disponibilidad de la información y los activos asociados a su tratamiento independiente de la forma en la que la información se encuentre.

cc) **Sistema de Gestión de Seguridad de la Información:** Es un componente del sistema de gestión de una organización, con base en un enfoque de riesgos, que tiene como función establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. El SGSI está conformado por políticas, procedimientos, directrices, recursos y actividades asociadas, gestionadas por la organización, en la búsqueda de la protección de sus activos de información.

dd) **Teletrabajo:** El teletrabajo consiste en la prestación de servicios subordinada, sin presencia física en el PRONABEC, a través de medios informáticos, de telecomunicaciones y análogos, mediante los cuales, a su vez, se ejerce el control y la supervisión de las labores.

ee) **Token:** Dispositivo de almacenamiento criptográfico que contiene el Certificado Digital asignado a la persona titular del mismo, que le permite firmar digitalmente.

ff) **Trabajo remoto**: El trabajo remoto consiste en la prestación de servicios subordinada con la presencia física del trabajador en su domicilio o lugar de aislamiento domiciliario, utilizando cualquier medio o mecanismo que posibilite realizar las labores fuera del centro de trabajo, siempre que la naturaleza de las labores lo permita. Este no se limita al teletrabajo, sino que se extiende a cualquier tipo de trabajo que no requiera la presencia física del trabajador en el centro de labores.

gg) **Usuario:** persona que hace uso de un recurso informático o servicio de tecnología de la información para fines laborales.

hh) **Video a demanda:** Corresponde a los portales de Video/Audio a demanda y en vivo por internet como Youtube, Vimeo, Spotify, etc. o canales de radio y televisión por internet.

ii) **Vulnerabilidad:** Debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad o disponibilidad de dicho activo.

6. SIGLAS

- **CGD:** Comité de Gobierno Digital del PRONABEC
- **MINEDU:** Ministerio de Educación
- **NTP:** Norma Técnica Peruana
- **OAF:** Oficina de Administración y Finanzas
- **OAGD:** Oficina de Atención al Ciudadano y Gestión Documentaria
- **OAJ:** Oficina de Asesoría Jurídica
- **OGTA:** Oficina de Gestión del Talento
- **OITEC:** Oficina de Innovación y Tecnología
- **PRONABEC:** Programa Nacional de Becas y Crédito Educativo
- **SGSI:** Sistemas de Gestión de la Seguridad de la Información
- **TI:** Tecnologías de la Información

7. DISPOSICIONES GENERALES

El PRONABEC gestiona, mantiene, monitorea, documenta y efectúa el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI) mediante su Comité de Gobierno Digital (CGD) y promueve el cumplimiento de normas técnicas, estándares internacionales y de las mejores prácticas de seguridad de la información, a fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

Por ello se establece las siguientes disposiciones generales:

a) Todo lo contenido en este documento es de aplicación obligatoria por parte de todo el personal bajo los distintos regímenes laborales del PRONABEC, las personas bajo contratos de locación y los proveedores que prestan servicios al PRONABEC.
b) Toda información interna (generada por el PRONABEC9 o externa (de propiedad de terceros) contenida en equipos informáticos, en medios físicos o digitales o en sistemas de información del PRONABEC, están bajo custodia de la Entidad y por lo tanto deberán ajustarse a la presente Directiva de seguridad de la información.
c) Toda información que se intercambie con otras Instituciones públicas o privadas, deberá ser tratada conforme a los acuerdos de confidencialidad que se encuentren establecidos en la Entidad.
d) Todo responsable de la dirección del órgano o unidad orgánica deberá asegurar que el personal a su cargo conozca los niveles de sensibilidad y criticidad de la información que se maneja en su unidad.
e) Todo personal deberá utilizar los recursos informáticos y/o sistemas de información puestos a su disposición, de manera legal, profesional y ética.
f) Todo personal deberá aplicar las disposiciones de seguridad física, es decir prevenir accesos no autorizados, daños en las instalaciones y resguardar los equipos ubicándolos en áreas protegidas con controles de acceso adecuados.
g) La presente Directiva deberá ser revisada al menos una vez por año para garantizar su vigencia y deberá mantener actualizada toda la documentación necesaria para dar cumplimiento.

8. DISPOSICIONES ESPECÍFICAS

8.1. Relativa a la organización de la Seguridad de la Información

El PRONABEC busca establecer un marco de referencia para la implementación, gestión y operación de la Seguridad de la Información dentro de la Entidad.

8.1.1. Segregación de funciones

El CGD debe segregar funciones para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos de información de la organización, así como para garantizar la protección de los activos de información y la gestión de riesgos de Seguridad de la Información.

8.1.2. Gestión de servicios y proyectos de Tecnologías de la Información (TI)

La OITEC debe integrar la seguridad de la información en sus procesos de gestión de servicios y proyectos de TI, para garantizar que los riesgos de seguridad de la información sean identificados y tratados pertinentemente.

8.1.3. Dispositivos móviles

El PRONABEC permite el uso de dispositivos móviles dentro y fuera de la infraestructura de comunicaciones de la Entidad, ya sean estos bienes de propiedad del PRONABEC o

bienes personales autorizados, donde toda información de la entidad que se almacena, transfiere o procesa siguen perteneciendo al PRONABEC por lo que la entidad mantiene el derecho a controlar dicha información, aunque no sea propietaria del dispositivo.

Obligaciones:

a) La OITEC debe gestionar el proceso de habilitación de los dispositivos móviles incluyendo su administración, instalación de aplicaciones, configuración de seguridad y asistencia técnica.
b) El usuario de un dispositivo móvil de propiedad privada (personal) debe solicitar autorización a su jefe inmediato para su uso dentro de la infraestructura de comunicaciones del PRONABEC.

Prohibiciones:

a) El personal del PRONABEC no debe utilizar los dispositivos móviles para uso distinto a las actividades laborales.
b) El personal del PRONABEC no debe permitir el acceso y uso de su dispositivo móvil por parte de otras personas no autorizadas ni debe transferir información del PRONABEC a otros dispositivos personales.

8.1.4. Teletrabajo y trabajo remoto

El PRONABEC permite el uso del teletrabajo y trabajo remoto para habilitar la ejecución de funciones del personal mediante el uso de equipos informáticos fuera de la Entidad, ya sean estos bienes de propiedad del PRONABEC o bienes personales autorizados, donde toda información que se almacena, transfiere o procesa siguen perteneciendo al PRONABEC por lo que la entidad mantiene el derecho a controlar esos datos, aunque no sea propietaria del dispositivo.

Obligaciones:

a) La OAF, mediante la Unidad de Abastecimiento, debe gestionar la habilitación de los equipos informáticos en el esquema de teletrabajo, de acuerdo a los requerimientos remitidos por las áreas usuarias y la disponibilidad presupuestal de la Entidad.
b) La OITEC debe gestionar la administración e instalación de software y aplicaciones, la configuración de seguridad y la asistencia técnica para los equipos informáticos utilizados en el esquema de trabajo remoto.
c) La OITEC debe aplicar el mecanismo de conexión remota segura mediante VPN o similar.
d) El usuario debe de asegurar que dispone de un entorno de trabajo adecuado y seguro para proteger el equipo y las credenciales de acceso a los sistemas e información de los que es responsable.

8.2. Seguridad relativa a los recursos humanos

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

8.2.1. Previo al vínculo laboral

Obligaciones:

a) La OGTA debe verificar los antecedentes laborales de la persona seleccionada y las competencias requeridas para el puesto.
b) La OGTA debe establecer en el Contrato Administrativo de Servicios, las cláusulas de confidencialidad de la información, de derecho de autor y de protección de datos personales, según corresponda.
c) La OGTA debe informar a la persona seleccionada de las responsabilidades administrativas y judiciales por el no cumplimiento de las disposiciones de la Seguridad de la Información.

8.2.2. Durante el vínculo laboral

Obligaciones:

a) La OGTA debe fortalecer el compromiso del personal con la Seguridad de la Información a través de programas de inducción para el personal que se vincule a PRONABEC, así como actualizaciones regulares de corresponder.
b) La OGTA debe coordinar con el Oficial de Seguridad de la Información, los contenidos de inducción y capacitación sobre seguridad de la información, incluyendo políticas, normas y directivas sobre la materia.
c) La OGTA debe comunicar al personal sus responsabilidades con respecto a la Seguridad de la Información según las funciones o actividades que realicen.
d) La OGTA debe comunicar a la OITEC, el inicio o rotación del vínculo laboral del personal para el otorgamiento de los correspondientes accesos a los sistemas de información, con una anticipación no menor a dos (2) días hábiles a la fecha prevista para el inicio de las labores del personal.
e) La OITEC debe ejecutar la “alta” efectiva de los accesos a las aplicaciones, grupos de colaboración y sistemas de información con un (1) día hábil de anticipación a la fecha prevista para el inicio de las labores del personal.
f) La OGTA comunica a la Secretaría Técnica de los Procedimientos Administrativos Disciplinarios, los actos que suponen el incumplimiento de las disposiciones de seguridad de la información establecidos en el presente instrumento, a fin que se lleve a cabo la precalificación de la supuesta conducta infractora y de ser el caso se disponga el inicio del Procedimiento Administrativo Disciplinario.

8.2.3. Al término del vínculo laboral

Obligaciones:

a) La OGTA debe comunicar a la OITEC, la finalización del vínculo laboral del personal para la baja de accesos correspondiente, con una anticipación no menor a un (1) día hábil a la fecha prevista para la extinción del vínculo laboral.
b) La OGTA debe comunicar inmediatamente a la OITEC, en los casos en los cuales los órganos y/o unidades orgánicas informen sobre ceses o renuncias autorizadas el mismo día, sin considerarse la comunicación previa de un (01) día de antelación.
c) La OITEC debe ejecutar la “baja” efectiva de los accesos a las aplicaciones, grupos de colaboración y sistemas de información el último día del periodo del vínculo laboral del personal.

8.3. Seguridad relativa a los activos de información

8.3.1. Inventario de activos de información

Obligaciones:

a) La OITEC debe mantener un inventario de activos de sistemas de información actualizado semestralmente.
b) La OAF, mediante la Unidad de Abastecimiento, debe mantener un inventario de equipos informáticos actualizado y revisado semestralmente.

8.3.2. Uso de activos de información

Obligaciones:

a) Todo personal debe usar los activos de información para los fines y objetivos del PRONABEC, bajo el criterio de buen uso y de acuerdo con las normas, políticas y procedimientos que se definan en la Entidad.
b) Todos los órganos y unidades orgánicas del PRONABEC deben cumplir con los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo la presente Directiva.
c) Todos los órganos y unidades orgánicas del PRONABEC deben inscribir aquellos activos de información (banco de datos) que estén amparados bajo la Ley de Protección de Datos Personales ante la Dirección General de “Transparencia, Acceso a la Información Pública y Protección de Datos Personales”, de acuerdo al reglamento de registro de la mencionada ley; asimismo deberán cumplir y mantener actualizado el inventario de sus activos de información, así como su clasificación y ponderación tomando en cuenta la directiva de Seguridad de la Información administrada por los Bancos de Datos Personales.
d) En el marco de las relaciones que el PRONABEC establezca con terceros, mediante orden de servicio, convenios y contratos, deben de consignarse cláusulas o disposiciones referidas a la confidencialidad de la información, así como sobre la cesión de derechos, de corresponder.
e) Solo podrán desempeñar sus funciones y actividades laborales utilizando los equipos informáticos administrados por el PRONABEC, ya sean estos asignados por la Unidad de Abastecimiento de la OAF, provistos por medio de un servicio contratado y excepcionalmente, con equipos personales previamente autorizados

8.3.3. Retorno de activos de información

Obligaciones:

a) La OAF, a través de la Unidad de Abastecimiento, debe supervisar el retorno de los equipos informáticos de la Entidad, asignados a los servidores que se desvinculan laboralmente del PRONABEC.
b) La OAF, a través de la Unidad de Abastecimiento, debe notificar a la OITEC respecto a cada equipo de cómputo retornado para las acciones de preparación previa a una nueva asignación.
c) La OGTA debe de establecer el procedimiento para el retorno de los activos de información correspondiente a expedientes documentales de la Entidad de los servidores que se desvinculan laboralmente del PRONABEC.

8.3.4. Clasificación de la información

Obligaciones:

a) Todo personal debe considerar que toda información que posea el PRONABEC es de acceso PÚBLICO, salvo las excepciones previstas en los artículos 15, 16 y 17 del Texto Único Ordenado de la Ley N°. 27806 - Ley de Transparencia y Acceso a la Información Pública, aprobado por Decreto Supremo N° 021-2019-JUS.
b) El acceso a información PÚBLICA está sujeto a los procedimientos dispuesto por establecidos en el Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública, y su Reglamento.
c) Los propietarios de activos de información deben de clasificar la información que generan en cada proceso y/o proyecto, de acuerdo a los criterios establecidos en el Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública.
d) Los propietarios de activos de información deben de etiquetar la información únicamente en caso de resultar clasificadas como CONFIDENCIAL o RESERVADA, así mismo, dicha clasificación debe ser notificada al Oficial de Seguridad de la Información para su registro en los inventarios correspondientes.
e) No está permitido el traslado, la divulgación y exposición de la información clasificada como CONFIDENCIAL o RESERVADA.
f) Toda desclasificación de información se hará cumpliendo lo señalado en la Ley de Transparencia y Acceso a la Información Pública y su Reglamento.
g) Todo personal debe velar por la conservación y custodia de toda información.
h) Todo personal que tenga acceso a información CONFIDENCIAL o RESERVADA debe ser consciente de la sensibilidad de la información que manejan y comprender a detalle sus responsabilidades relacionadas con la protección de la información.
i) Los registros de información, que se encuentren documentados en papel, o medios electrónicos y tecnológicos deben estar almacenados y resguardados en una zona segura con acceso limitado a las personas no autorizadas.

8.3.5. Gestión de medios removibles

Obligaciones:

a) La OITEC debe establecer el procedimiento para la gestión de medios removibles considerando las labores realizadas por los servidores de acuerdo a la necesidad de uso.
b) La OITEC debe establecer los controles a las transferencias de información externas por medios físicos, manteniendo lineamientos para los servicios de mensajería y transporte de información en distintos soportes.

8.3.6. Disposición o reutilización segura de equipos y medios

Obligaciones:

a) La OITEC debe establecer y ejecutar los procedimientos para la disposición de los datos e información almacenados en los equipos informáticos y medios removibles a ser destruidos, donados o transferidos a un nuevo usuario.
b) La OITEC debe orientar a todo el personal respecto a su responsabilidad de mantener una copia de resguardo de los datos e información almacenados en los equipos de computación previo a su eliminación.
c) La OITEC debe solicitar la autorización a la jefatura de los órganos o unidades orgánicas correspondiente, para la eliminación de datos e información en equipos de cómputo que, por el uso posterior que se les den, requieran de dicha acción.
d) Toda información almacenada en soportes externos (CD, DVD, unidades USB, tarjetas de memoria y papel) y en todos los equipos que tienen soporte de almacenamiento interno (equipos de cómputo, teléfonos móviles) deben ser

borrados (formateado), o se debe destruir el soporte, antes de ser eliminados o reutilizados.

e) La destrucción de información CONFIDENCIAL o RESERVADA debe realizarse por medios o mecanismos que no permitan su regeneración bajo ninguna circunstancia.

8.4. Seguridad relativa al control de accesos

8.4.1. Gestión de acceso a recursos de información y estaciones de trabajo

Obligaciones:

a) La OITEC debe establecer los procedimientos formales para asignar los derechos de acceso a los recursos de información relacionados con los servicios de TI y sistemas de información.
b) La OITEC debe implementar los controles necesarios para garantizar la autenticación y el acceso a los recursos de información relacionados con los servicios de TI y sistemas de información.
c) La OITEC debe gestionar el acceso a las estaciones de trabajo a fin de evitar accesos no autorizados a recursos o activos de información.
d) La OITEC debe verificar semestralmente que los usuarios tengan acceso permitido únicamente a aquellos recursos de información para los que fueron autorizados.
e) Los responsables de direcciones y unidades deben solicitar a la OITEC la alta y baja de accesos a los servicios de TI, sistemas de información para el personal, locadores y proveedores de servicios a su cargo, indicando los niveles de acceso o privilegios.
f) La OITEC debe establecer las pautas para la asignación y cambio de contraseñas.
g) La OITEC debe generar, a la comunicación del inicio de vínculo laboral de los servidores por parte de la OGTA, las credenciales de acceso que identifique única y exclusivamente al servidor para el uso de los siguientes servicios de TI y sistemas de información:
   - acceso al Dominio
   - acceso a Intranet del Colaborador y SIGEDO
   - acceso al Correo electrónico institucional y herramientas colaborativas
h) La OITEC debe garantizar la aplicación de buenas prácticas de seguridad en cuanto a la elección y uso de contraseñas considerando que todo personal:
   - Debe utilizar contraseñas con una secuencia de caracteres con al menos ocho caracteres de longitud, considerando contener como mínimo, un carácter numérico, un carácter alfabético en mayúscula y uno en minúscula.
   - Debe cambiar su contraseña si existe un indicio de que haya sido vulnerado o estar en riesgo un activo de información (en ese caso, se debe reportar el incidente de seguridad).
   - Debe cambiar las contraseñas por cada periodo de 3 meses o 90 días.
   - Debe cambiar las contraseñas generadas por defecto en el primer ingreso a un sistema de información.
   - No debe considerar información relacionada directamente con el usuario (nombre, fecha de nacimiento, DNI, etc.)
   - No debe revelar las contraseñas a otras personas, incluyendo al personal de asistencia técnica de la OITEC y a los administradores de los sistemas de información.
   - No debe transferir o distribuir su contraseña por ningún medio (oral, escrito, electrónico, etc.) por ser estrictamente personal y de su responsabilidad.

- No debe llevar un registro de las contraseñas, a menos que se realice en un documento debidamente cifrado o encriptado mediante una contraseña que cumpla los niveles de complejidad descritos en el presente documento.
- No debe considerar el uso de las últimas dos contraseñas pasadas como nueva contraseña
- No debe almacenar contraseñas en un sistema de registro automatizado (por ej., macros o explorador).

8.4.2. Control de acceso a las redes de comunicaciones

Obligaciones:

a) El acceso a las redes de comunicaciones y recursos de red internos y externos debe ser gestionado por la OITEC de manera que el personal no comprometa la seguridad de los activos de información.
b) El control de acceso debe tener en cuenta los siguientes aspectos:

- Segmentación de las redes (personal de PRONABEC o visitantes)
- Tipo de red de comunicación (red de datos, telefonía fija, telefonía móvil)
- Ubicación de usuario (acceso local o acceso remoto)
- Modalidad de conectividad a red de datos (Cableada o inalámbrica)

8.4.3. Control de acceso en los sistemas de información

Obligaciones:

a) La OITEC debe establecer e implementar las pautas de control de acceso a los sistemas de información que garanticen la restricción efectiva para uso exclusivo del personal debidamente autorizado.
b) La OITEC debe gestionar el control de acceso, siempre que cuente con los mecanismos para controlar los accesos del sistema de información y mediante los administradores de los sistemas de información, quienes además de llevar un registro de accesos autorizados, deben revisar semestralmente los accesos concedidos, revocando los derechos de cuya vigencia de autorización haya caducado.
c) La OITEC debe informar a los usuarios sobre las responsabilidades a la que conlleva los accesos provistos y la obligatoriedad de la confidencialidad y cambio de contraseña de acuerdo a la disposición establecida.
d) La OITEC debe implementar mecanismos físicos o lógicos para realizar el aislamiento o resguardo de sistemas de información con información sensible.

8.4.4. Gestión de derecho de acceso remoto

Obligaciones:

a) La OITEC debe establecer e implementar los mecanismos para permitir el acceso remoto mediante el uso de tecnología de acceso seguro como la VPN y mecanismos de autenticación con credenciales de accesos únicos.
b) La OITEC debe establecer los procedimientos para la asignación, uso y revocación del derecho de acceso remoto, el cual debe considerar la autorización del jefe inmediato y justificación de la necesidad.
c) La OITEC debe notificar cada habilitación de acceso remoto al Oficial de Seguridad de la Información para su correspondiente registro.
d) La OITEC debe gestionar y controlar otros mecanismos de acceso o conexión remota no autorizados o institucionales, incluyendo el uso de herramientas y software de escritorio o terminal remoto (Anydesk, Teamviewer, etc.).

8.4.5. Gestión de derechos de acceso privilegiado

Obligaciones:

a) La OITEC debe establecer los procedimientos para la asignación, uso y revocación de los derechos de accesos privilegiados, el cual debe considerar la autorización del jefe inmediato y justificación de la necesidad.
b) El control de acceso privilegiado debe ser gestionado por la OITEC.
c) Los derechos de acceso privilegiado sólo deben ser otorgadas al personal de nivel técnico apropiado y únicamente para el cumplimiento de sus funciones.
d) Los accesos realizados con credenciales de acceso privilegiados deben ser registrados y controlados periódicamente.
e) Una credencial de acceso privilegiado sólo debe ser utilizada en la actividad de administración o configuración del sistema para la cual se requieren dichos privilegios.
f) Una credencial de acceso privilegiado no debe ser utilizada en actividades rutinarias para la que exista un perfil de menores privilegios que lo permita.
g) Las credenciales de acceso privilegiadas tales como “administrador”, “root” o similares que son definidas por defecto en los sistemas y componentes, no deben ser utilizadas siempre que sea posible generar cuentas de acceso privilegiados.
h) Se debe asegurar con contar con un mecanismo de recuperación de acceso privilegiado
i) El acceso privilegiado debe realizarse desde dispositivos debidamente fortalecidos para tal fin.

8.5. Seguridad relativa a la criptografía

Obligaciones:

a) La OITEC debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión interna o externa de información, cuente con mecanismos de cifrado de datos, asimismo, deberá solicitar a los proveedores de servicios de comunicación y transmisión de datos que cumplan con lo señalado en este párrafo.

8.6. Seguridad relativa a las instalaciones y el entorno físico

La seguridad en las instalaciones y el entorno físico se alcanza mediante la adopción de medidas destinadas a prevenir, detectar, neutralizar y/o disminuir los riesgos que la amenazan, las mismas que se basan en el convencimiento de que no hay ningún peligro que temer al haberse adoptado las medidas necesarias para evitar todo riesgo.

8.6.1. Áreas físicas

Obligaciones:

a) La OITEC y la OAF, a través de la Unidad de Abastecimiento, deben clasificar las áreas físicas para definir el nivel de seguridad de las mismas, las cuales se describen como sigue:

Clasificación	*Etiqueta*	*Definición*
Pública	**AREA PÚBLICA**	Aquella zona que es de uso público y de recepción de personas externas (visitantes) a la Entidad.
Común	**AREA COMÚN**	Aquella zona de uso común para los servidores del PRONABEC.
Restringida	**AREA RESTRINGIDA**	Aquella zona donde la información que se genera, trata o almacena es crítica para el PRONABEC. El acceso a este tipo de zonas requiere autorización y/o un control acceso.

b) Cada órgano o unidad orgánica, que sea responsable de un área física clasificado como restringida, debe implementar los controles necesarios para garantizar un acceso autorizado a dichos espacios físicos y las medidas de protección contra amenazas externas y ambientales considerando los siguientes, de corresponder:
   - Control de acceso
   - Video vigilancia y seguridad física
   - Control de humedad
   - Detectores de incendio o humo
   - Extintores o sistema de extinción de fuego
   - Sistema de puesta o pozo a tierra
   - Sensores de aniegos
   - Sistema de alimentación ininterrumpida (UPS)
   - Grupo electrógeno
   - Pararrayos

c) Cada órgano o unidad orgánica, que sea responsable de un área física clasificado como restringida, deben verificar semestralmente que los usuarios tengan acceso permitido únicamente a aquellas áreas para los que fueron autorizados.

d) El acceso a un área física clasificada como restringida está permitido para personas externas al PRONABEC, siempre que sea para un motivo específico, que se cuente con la autorización respectiva del jefe inmediato responsable del área en cuestión y debe estar siempre acompañado por un personal del PRONABEC.

e) Las áreas restringidas deben de contar con un circuito cerrado de video, sistema de video vigilancia o equivalente.

f) El Centro de Datos es una zona restringida y la OITEC debe implementar los controles de acceso para su debida protección.

g) La OITEC debe proteger el Centro de Datos de fallas por falta de suministro de energía y otras anomalías eléctricas.

8.6.2. Equipos de cómputo

Obligaciones:

a) La OAF, a través de la Unidad de Abastecimiento, debe autorizar las solicitudes de traslados de bienes y/o activos a otra ubicación.

b) La OAF, a través de la Unidad de Abastecimiento y la OITEC deben garantizar la protección de los equipos informáticos de fallas por falta de suministro de energía y otras anomalías eléctricas.

c) La OITEC debe garantizar la protección del cableado de la red de datos y los equipos de comunicaciones de fallas por falta de energía o protección física.

d) La OITEC debe brindar mecanismos necesarios para proteger la confidencialidad, integridad y disponibilidad de los equipos de cómputo dentro y fuera de las instalaciones del PRONABEC.

e) La OITEC debe mantener un plan de mantenimiento preventivo de la infraestructura tecnológica incluyendo los equipos de cómputo, escaneo, impresión y servidores del Centro de Datos a fin de para garantizar la continuación de los servicios.

f) La OAF, a través de la Unidad de Abastecimiento y la OITEC deben mantener un plan de mantenimiento preventivo de los equipos de acondicionamiento de temperatura, humedad, filtrado de aire, sistemas de energía ininterrumpida (UPS) y detección o extinción de fuego a fin de garantizar su operatividad.
g) La OITEC y su personal de asistencia técnica son los únicos autorizados para realizar instalaciones y configuraciones de los equipos de cómputo, escaneo e impresión.

8.6.3. Equipos de usuarios desatendido

Obligaciones:

a) La OITEC debe promover y orientar a los usuarios respecto al procedimiento de bloqueo de sesión de sus equipos de cómputo cuando no se encuentren en su lugar de trabajo. Esto con el fin que la sesión del usuario no quede activa para evitar el uso inadecuado de terceros.

8.6.4. Pantalla y escritorio limpio

Obligaciones:

a) La OITEC debe orientar al personal respecto a mantener el escritorio del equipo de cómputo libre de información de uso interno propia de la institución, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
b) La OITEC debe garantizar el bloqueo de la pantalla de un computador administrada por el PRONABEC para forzar un nuevo inicio de sesión, si la persona se ausenta del computador por un período de mínimo de 5 minutos.
c) La OITEC debe garantizar el cierre de toda sesión activa de un usuario en los sistemas de información institucionales para obligar un nuevo inicio de sesión, indistintamente si se encuentra en un computador administrado por PRONABEC o no, siempre que la persona no tiene actividad en el sistema de información por un período de 5 minutos.
d) La OITEC debe considerar el apagado del computador si el tiempo de ausencia es superior a los 90 minutos.
e) Toda la información clasificada como CONFIDENCIAL y RESERVADA, ya sean documentos impresos o soportes de almacenamiento, es considerada sensible y no deben estar expuestos en el escritorio del puesto de trabajo u otras zonas de trabajo (incluyendo impresoras y fotocopiadoras) para evitar el acceso no autorizado a los mismos.

8.7. Seguridad relativa a las operaciones

El PRONABEC debe contar con mecanismos para asegurar que sus operaciones e instalaciones de procesamiento de la información sean correctas y seguras, mitigando los riesgos de seguridad como las intrusiones no autorizadas y ejecución de código malicioso dentro de la infraestructura tecnológica del PRONABEC.

8.7.1. Procedimientos operativos documentados

Obligaciones:

a) La OITEC debe mantener actualizados los procedimientos relacionados con la operación y administración de seguridad de la infraestructura tecnológica que soporta los sistemas de información, estableciendo responsabilidades y los recursos utilizados para su ejecución eficiente, asimismo, estos deben estar a disposición del personal autorizado.

b) La OITEC debe mantener actualizada la documentación relacionada con los manuales de configuración, operación y uso de los sistemas de información e la Entidad.

8.7.2. Gestión de cambios

Obligaciones:

a) La OITEC debe mantener un registro de control de cambios de los sistemas de información, los equipos de comunicaciones, el centro de datos y bases de datos a través de la implementación de acciones y procedimientos orientados a asegurar que todo cambio siga un proceso planificado que incluya responsabilidades y canales de comunicación, identificación de los recursos comprometidos, pruebas de estrés, validación de controles de seguridad, reversión en caso de fallas y análisis de impacto.
b) Todo cambio debe ser solicitado a la OITEC por el propietario de la información, y se llevara un registro sobre cada solicitud de cambio. En caso se presente un problema con el cambio realizado, se revertirá al estado anterior al cambio.

8.7.3. Gestión de la capacidad

Obligaciones:

a) La OITEC debe garantizar la capacidad de los recursos a fin de asegurar el óptimo desempeño y la continuidad de los sistemas de información y la infraestructura tecnológica que la soporta.
b) La OITEC debe realizar estudios sobre las proyecciones de crecimiento de los recursos administrados de manera periódica, con el fin de asegurar el desempeño y capacidad de la infraestructura tecnológica.
c) La OITEC debe realizar un monitoreo continuo del uso de sus capacidades para advertir eventos e incidencias relacionadas.

8.7.4. Separación de entornos de desarrollo de software

Obligaciones:

a) La OITEC debe separar los entornos de desarrollo, control de calidad, aceptación de usuario y producción a fin de garantizar el mejor desempeño requerido por los sistemas de información durante todo su ciclo de vida.
b) La OITEC debe gestionar los recursos necesarios para la implantación de controles que permitan la separación de entornos.

8.7.5. Protección contra software y código malicioso:

El PRONABEC proporciona los mecanismos necesarios para garantizar la protección de la información y el equipamiento informático donde se procesa y almacena la información contra el hurto, modificación o daño ocasionados por el contagio de software malicioso.

Obligaciones:

a) La OITEC debe gestionar los controles para garantizar la prevención, detección y eliminación de software y código malicioso en todo equipo informático del PRONABEC.
b) La OITEC debe asegurar que todas las estaciones de trabajo cuenten con el software antivirus y que estos se encuentren debidamente actualizados a fin de prevenir la ejecución de software malicioso.

c) La OITEC debe asegurarse que todas las aplicaciones y sistemas operativos se encuentren actualizados a fin de que minimicen los riesgos por vulnerabilidades.
d) La OITEC debe proveer asistencia técnica y ejecutar medidas de control frente a los reportes de incidentes de usuarios.

8.7.6. Respaldo de información

Obligaciones:

a) La OITEC debe establecer los procedimientos rutinarios para la generación y restauración de copias de respaldo de los sistemas de información hospedadas en el centro de datos del PRONABEC.
b) La OITEC debe clasificar y etiquetar las copias de respaldo que le permita la fácil identificación de los medios de almacenamiento, la información contenida y la ubicación física para su posterior ubicación y acceso a los medios que contienen la información resguardada del centro de datos.
c) La OITEC debe registrar las operaciones de respaldo ejecutadas.
d) La OITEC debe realizar pruebas de restauración en base a las copias de respaldo a fin de garantizar la recuperación de información en el momento de ser necesaria.
e) La OITEC debe establecer las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información de ser almacenadas externamente.
f) La OITEC debe evaluar periódicamente la vigencia tecnológica de la infraestructura de hardware y software utilizados para el respaldo y recuperación de la información.
g) La OITEC debe establecer los procedimientos para el almacenamiento y resguardo de información de las estaciones de trabajo de los usuarios para que se soporten bajo el servicio de almacenamiento en nube del PRONABEC.

8.7.7. Registro y Monitoreo

Obligaciones:

a) La OITEC debe generar los registros de eventos de los sistemas de información tal como la activación de registros de auditoría, registros de uso de recursos y de conexiones.
b) La OITEC debe realizar un monitoreo de los registros para seguimiento e investigación de incidencias presentadas.
c) La OITEC debe gestionar los accesos a los repositorios de registros.
d) Todos los servicios de TI y sistemas de información deben estar sujetos a un monitoreo por parte de la OITEC.

8.7.8. Sincronización de reloj

Obligaciones:

a) La OITEC debe mantener la sincronización de los relojes de toda su infraestructura tecnológica, incluyendo a los equipos informáticos y sistemas de información.
b) La OITEC debe utilizar como fuente de tiempo referencial a la establecida como la “Hora Oficial de la República del Perú”.
c) La OITEC debe asegurarse de la inviolabilidad del cambio de hora de los equipos por parte del personal del PRONABEC.

8.7.9. Control de software operacional

Obligaciones:

a) La OITEC debe implementar los mecanismos de restricción para la instalación de software en los equipos de cómputo.
b) La OITEC debe restringir y limitar el otorgamiento de privilegios para la instalación de software en los equipos de cómputo del PRONABEC.
c) La OITEC debe autorizar todo software previo a su instalación en equipos de cómputo del PRONABEC, así mismo es responsable por la validación del licenciamiento de corresponder para evitar el incumplimiento de uso ilegal de software.

8.8. Seguridad relativa a las comunicaciones

El PRONABEC debe contar con mecanismos para asegurar las redes de comunicaciones y la infraestructura que la soporta, mitigando los riesgos de seguridad como las intrusiones no autorizadas e interceptaciones de información tanto dentro como fuera de la Entidad.

8.8.1. Acceso al dominio PRONABEC

Obligaciones:

a) La OITEC debe establecer los procedimientos para la asignación, uso y revocación de las cuentas de dominio.
b) La OITEC debe asegurar que los equipos de cómputo cuenten con adherencia al dominio PRONABEC a fin de garantizar el uso de cuentas de dominio como mecanismo de autenticación y control de acceso. En caso no sea posible la adherencia se debe optar por el uso de grupo de trabajo PRONABEC.
c) La OITEC debe asignar una cuenta de dominio individual al personal del PRONABEC, la cual debe permitir el inicio de sesión en un equipo de cómputo.
d) La cuenta de dominio asignada es de carácter individual, por consiguiente, ningún otro usuario debe utilizar una cuenta de dominio que no sea la suya.
e) La OITEC debe gestionar la asignación de cuentas de dominio para terceros cuando se requiera el acceso de personal externo a los equipos informáticos y servicios de TI del PRONABEC. Una cuenta de dominio para terceros debe ser autorizado por los directores de Oficina y de Unidad quienes se responsabilizan de la custodia y uso del mismo.
f) El uso del dominio y las redes de comunicación interna debe estar restringido para realizarse mediante el uso de equipos de cómputo bajo la gestión del PRONABEC. El uso de dispositivos móviles personales será posible únicamente bajo autorización previa.
g) El acceso remoto, requerido para los esquemas de tele-trabajo o acceso a servicios internos, debe ser efectivo mediante el uso de las cuentas de dominio asignadas.

8.8.2. Acceso a internet

Obligaciones:

a) La OITEC debe garantizar la protección del servicio de internet contra ataques de intrusiones o denegación de servicio, así como el acceso a páginas no autorizadas.
b) La OITEC debe promover la concientización a los usuarios respecto a las consideraciones de seguridad que deben adoptar para el adecuado uso del internet.
c) La OITEC debe realizar el monitoreo de los servicios prestados por los proveedores a fin de asegurarse la adecuada provisión y operatividad de los servicios acordados.
d) La OITEC debe supervisar las medidas de seguridad implementadas por parte de los proveedores de servicio.

e) El acceso a Internet es un servicio de TI que está disponible para todo el personal del PRONABEC para uso estricto de actividades laborales relacionadas con las funciones que desempeñan y no para uso con propósitos de índole personal o comercial.
f) La OITEC debe habilitar el acceso a internet con navegación básica que permita el acceso a portales web con dominios relacionados a educación, gobierno, cultura, salud, política y economía, así como permitir el acceso al servicio de correo electrónico institucional y a los sistemas de información del PRONABEC.
g) La OITEC puede habilitar accesos a internet con navegación especial previa autorización de los Directores de Oficina y de Unidad para que se permita el acceso a portales de redes sociales, video a demanda o a ambos. Los accesos habilitados estarán sujetos a controles y auditorias con la finalidad de garantizar el buen uso del servicio.
h) Las operaciones o actividades realizadas con el servicio de acceso a internet es de exclusiva responsabilidad del usuario exonerándose al PRONABEC de toda responsabilidad con respecto al uso del mismo.

8.8.3. Correos electrónicos

Obligaciones:

a) La OITEC debe asignar una cuenta de correo electrónico institucional a cada personal del PRONABEC, la cual debe permitir enviar y recibir correos electrónicos internos y externos a PRONABEC.
b) La OITEC puede asignar un buzón compartido cuando se requiera representar a un evento, un servicio o un sistema para enviar y recibir correos electrónicos internos o externos a PRONABEC.
c) La OITEC puede asignar una cuenta de correo genérica únicamente cuando se requiera la generación de una credencial (usuario y contraseña) de acceso independiente para representar a un evento, un servicio o un sistema que requiera enviar y recibir correos electrónicos internos o externos a PRONABEC.
d) La OITEC puede asignar una lista de distribución cuando se requiera el envío masivo de correos electrónicos a cuentas de correo electrónicos institucionales del PRONABEC de manera continua.
e) La OITEC puede asignar una cuenta de correo electrónico institucional a personas bajo contratos de locación y proveedores, la cual debe estar habilitada para enviar y recibir correos electrónicos internos y restringido para el envío de correos electrónicos externos a PRONABEC.
f) El uso del servicio de correo electrónico es de exclusiva responsabilidad del usuario titular de la cuenta exonerándose al PRONABEC de toda responsabilidad con respecto al uso del mismo.
g) El correo electrónico es para fines netamente laborales vinculadas a las funciones del personal y no debe permitir el envío de mensajes masivos a dominios públicos de internet.
h) La OITEC puede realizar la des-habilitación temporal o permanente de una cuenta de correo electrónico de evidenciarse un uso indebido que transgreda lo establecido en la presente directiva.
i) La OITEC debe garantizar la protección de las cuentas de correo electrónicos de accesos no autorizados, denegación de servicios o suplantación de identidad.
j) La OITEC debe promover la concientización a los usuarios respecto a las consideraciones de seguridad que deben adoptar para el adecuado uso y protección de los mensajes de correos electrónicos principalmente con la encriptación de mensajes durante el intercambio de información con destinatarios externos al PRONABEC.

8.8.4. Segmentación de las redes

Obligaciones:

a) La OITEC debe mantener una red de datos segmentada por redes virtuales, grupos de servicios, grupos de usuarios, ubicación física o cualquier otra tipificación que se considere conveniente en el PRONABEC, debiendo estar documentada en la arquitectura correspondiente.
b) La OITEC debe de segmentar la red de datos, sea esta cableada o inalámbrica, para aislar los accesos de visitantes de la red de datos del personal administrativo, de los servicios de TI y de los sistemas de información.
c) La OITEC debe implementar controles para minimizar los riesgos contra accesos no autorizados a la infraestructura de redes de comunicaciones interna y para salvaguardar la información de las estaciones de trabajo y los sistemas de información.

8.8.5. Transferencia de información

Obligaciones:

a) La OITEC debe establecer los controles a las transferencias e intercambios de información externas por medios físicos (medios removibles) y electrónicos (correos electrónicos, archivos compartidos o FTP) de tal manera que solo sea emitida y recibida íntegramente por las personas apropiadas y autorizadas en el momento y lugar oportuno.
b) La OITEC debe promover la concientización a los usuarios respecto a las consideraciones de seguridad que deben adoptar para el adecuado uso y protección de información clasificada como confidencial y sus restricciones para ser transferidas.

8.8.6. Acuerdos de confidencialidad o de no divulgación

Obligaciones:

a) La OAF y la OAJ deben establecer los Acuerdos de Confidencialidad y/o de entrega de información con terceras partes, según corresponda.
b) La OITEC debe establecer los procedimientos y controles necesarios para el intercambio de información y debe promover el uso de mecanismos seguros en tecnologías de la información y redes de telecomunicaciones.

8.9. Seguridad relativa a la adquisición, desarrollo y mantenimiento de sistemas

El PRONABEC debe asegurar que los sistemas de información cumplan con los requisitos de seguridad para evitar pérdidas, modificación o mal uso de la información que se procese en ellas, así como proteger la confidencialidad, autenticidad e integridad de la información.

8.9.1. Procesos y documentación de los Sistemas de Información

Obligaciones:

a) La OITEC debe establecer un procedimiento para la adquisición, desarrollo y mantenimiento de los sistemas de información.
b) La OITEC debe mantener la documentación de los sistemas de información desarrollados con la finalidad de garantizar la ejecución de sus actividades y la realización de mantenimiento posterior.

8.9.2. Requisitos de seguridad de los Sistemas de Información

Obligaciones:

a) La OITEC debe establecer en su metodología de desarrollo de software, los requerimientos de seguridad y buenas prácticas de desarrollo de software seguro, así como incluir el diseño de controles de seguridad durante las etapas de análisis y diseño de los sistemas de información.
b) La OITEC debe proporcionar a todo desarrollador de software las consideraciones elementales de seguridad de la información, controles, estándares y metodologías.
c) Todo sistema de información desarrollado por el personal del PRONABEC es de propiedad de la Entidad.
d) La OITEC debe verificar que los acuerdos con locadores o proveedores sobre materia de adquisición o desarrollo de sistemas, incluyan clausulas relativas a la cesión de derechos a favor del PRONABEC y confidencialidad de la información para el resguardo de la propiedad intelectual del PRONABEC.
e) La OITEC debe asegurarse que todo sistema de información, ya sea este adquirido o desarrollado, implemente los requisitos de seguridad establecidos y utilice los componentes de software debidamente licenciados.

8.9.3. Procesamiento correcto de los Sistemas de Información

Obligaciones:

a) La OITEC debe asegurarse de validar los datos de entrada, el procesamiento interno y los datos de salida mediante controles de seguridad.
b) La OITEC debe identificar los requerimientos para garantizar la autenticidad y la integridad de los datos en los sistemas de información.
c) La OITEC debe establecer tiempo de duración de las sesiones activas en los sistemas de información, terminándolas cuando se cumpla el tiempo de inactividad.
d) La OITEC debe implementar el uso de la encriptación y otros controles criptográficos que permitan proteger la confidencialidad, autenticidad e integridad de la información de acuerdo a su clasificación y nivel de exposición al riesgo.

8.9.4. Control de acceso al Código Fuente de los Sistemas de Información

Obligaciones:

a) La OITEC debe implementar controles para restringir y controlar el acceso al código fuente de los sistemas de información.
b) La OITEC debe gestionar el acceso a los repositorios de código fuente o de software desarrollado manteniendo un registro de uso.

8.9.5. Control de cambios de los Sistemas de Información

Obligaciones:

a) La OITEC debe gestionar el control cambio de los sistemas de información.
b) La OITEC debe gestionar un control de versiones de cada sistema de información.

8.9.6. Datos de prueba para los Sistemas de Información

Obligaciones:

a) La OITEC debe seleccionar, proteger y controlar los datos de pruebas de manera cuidadosa previos al uso de los sistemas de información.

b) La OITEC debe asegurar que los datos personales utilizados en los ambientes de desarrollo y de prueba sólo sean utilizados por el personal de desarrollo del aplicativo correspondiente, previa autorización del dueño (responsable) del banco de datos.
c) La OITEC debe asegurar de tomarse muestras (porción de los datos) de acuerdo a las metodologías de extracción de datos para las pruebas correspondientes por el área de desarrollo de software, así como las señaladas en la NTP ISO/IEC 12207.

8.9.7. Seguridad en los procesos de desarrollo y pase a producción

Obligaciones:

a) La OITEC debe asegurarse de que el desarrollo de los sistemas de información sea realizado conforme a los procedimientos establecidos en la NTP ISO/IEC 12207 y otros estándares similares.
b) La OITEC debe implementar controles para la puesta en práctica de procedimientos orientados a controlar el pase de sistemas de información desarrollados al entorno de producción.
c) La OITEC debe asegurar la disponibilidad y separación del entorno de desarrollo, entorno de control de calidad, entorno de aceptación de usuario y entorno de producción.
d) La OITEC debe garantizar una efectiva gestión de accesos a los entornos de producción previniendo accesos no autorizados por personal encargado del desarrollo y mantenimiento de sistemas de información.
e) Todo nuevo sistema de información o actualización desarrollada debe ser revisado previamente en los entornos de control de calidad y el de aceptación de usuario antes de su pase a producción.
f) El pase a producción mediante medios no automatizados debe ser realizado exclusivamente por el personal autorizado por la OITEC, quien debe de registrar su actividad en una bitácora.

8.9.8. Gestión de vulnerabilidades de seguridad

Obligaciones:

a) La OITEC debe realizar semestralmente pruebas de comprobación técnica para verificar que se cuenta con los controles de seguridad debidamente implementados.
b) La OITEC debe asegurarse de implementar las recomendaciones resultantes posteriormente a la identificación de vulnerabilidades de seguridad y debe de determinar los riesgos asociados e implementar los controles necesarios para mitigarlos. Los sistemas de información críticos y en alto riesgos deben ser priorizados.
c) La OITEC debe validar la efectividad de toda actualización propuesta en el entorno de control de calidad y debe cumplir con los controles establecidos para la gestión de cambios.

8.10. Sobre las relaciones con los proveedores

El PRONABEC debe garantizar la protección de sus activos de información accesibles por los locadores y proveedores.

8.10.1. Seguridad con relación a los proveedores

Obligaciones:

a) La OAF, a través de la Unidad de Abastecimiento, debe garantizar que todo proveedor de bienes y servicios suscriba un acuerdo de confidencialidad, el mismo que deberá ser parte del contrato.

b) La OAF, a través de la Unidad de Abastecimiento, debe de requerir al proveedor, los datos completos de las personas que interactuarán directamente con el PRONABEC, incluyendo las funciones y responsabilidades asociadas a las actividades a realizar, así como las actualizaciones de cambios de dicho personal (alta, baja o cambio de funciones o responsabilidades) que se presenten durante la ejecución contractual.
c) La OAF, a través de la Unidad de Abastecimiento, y las áreas usuarias, debe velar porque el proveedor y su personal cumpla con las consideraciones de seguridad aplicables de la presente Directiva.
d) El PRONABEC puede suministrar al proveedor de bienes y servicios información confidencial, relacionada con sus actividades, productos, servicios y/o su estrategia operativa únicamente si cuenta con una autorización previa por parte del propietario de dicha información.
e) La OAF, a través de la Unidad de Abastecimiento, debe incluir las siguientes cláusulas en el contrato de bienes y servicios menores o iguales a 8 UIT:

   i. Todo intercambio de información que se realice entre el PRONABEC y el proveedor tendrá la clasificación de confidencial y no podrá ser utilizada fuera de dicho marco de ejecución del servicio contratado. Toda información entregada por el PRONABEC seguirá siendo de propiedad de esta Entidad.
   ii. Todo proveedor debe considerar que toda información del PRONABEC a la que tenga acceso, puede estar sujeta a la Ley de Protección de Datos Personales.
   iii. Todo proveedor no debe utilizar la información del PRONABEC para beneficio propio o de terceros ni para fines distintos a los indicados en el contrato.

8.11. Seguridad relativa a la gestión de incidentes de seguridad de la información

El PRONABEC debe asegurar que los incidentes de seguridad de la información sean comunicados oportunamente a las instancias correspondiente con finalidad de adoptar acciones preventivas y correctivas que correspondan.

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

Obligaciones:

a) La OITEC debe realizar el registro de incidentes de la seguridad de la información reportados.
b) Los incidentes relativos a la seguridad de la información deben ser reportados a la OITEC, conforme al procedimiento que se establezca para tal efecto.
c) Se considerará como ataque a la seguridad de la información a cualquier actividad que se realice mediante la exploración y explotación de los recursos informáticos asignados por el PRONABEC siempre que estos se realicen sin la supervisión y/o autorización de la OITEC.
d) La OITEC debe realizar una evaluación permanente de los controles de seguridad existentes en sus sistemas de información para proponer mejoras para prevenir la ocurrencia de futuros incidentes de seguridad de la información.
e) La OITEC debe garantizar la generación de una base de conocimiento para la asistencia de incidentes de la seguridad de la información.

8.11.2. Respuesta a incidentes de seguridad de la información

Obligaciones:

a) La OITEC debe disponer de canales de comunicación que permitan que el personal reporte incidentes de seguridad, eventos sospechosos y el mal uso de los recursos informáticos.

b) La OITEC debe asistir al reporte de un incidente de seguridad como un primer nivel, pudiendo escalar a un nivel superior para la búsqueda de remediación, así como reportarlo al Oficial de Seguridad de la Información para la evaluación de la criticidad del incidente.
c) La OITEC debe asignar responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.
d) La OITEC debe considerar la identificación, recolección, preservación y análisis de evidencias, durante el tratamiento de los incidentes.
e) La OITEC debe reportar los incidentes identificados como masivos o recurrentes al Oficial de Seguridad de la Información y de requerirse podrán ser evaluados por el Comité de Gobierno Digital del PRONABEC a efectos de adoptar acciones correctivas y preventivas.

8.12. Seguridad relativa a la continuidad de servicios de TI

El PRONABEC busca preservar la integridad, confidencialidad y disponibilidad de la información durante un hecho o durante una situación adversa ya sean éstos por desastre natural u ocasionados por el hombre.

8.12.1. Continuidad de la seguridad de la información

Obligaciones:

a) La OITEC debe incluir la continuidad de la seguridad de la información dentro del proceso de gestión de continuidad operativa para actuar de manera efectiva ante algún posible evento que pudiera afectar la disponibilidad de la información.
b) La OITEC debe validar la efectividad de los controles de continuidad de la seguridad de la información que se han implementado.

8.12.2. Redundancias

Obligaciones:

a) La OITEC debe mantener redundancia a nivel de enlace de telecomunicaciones, servidores, base de datos y los otros recursos tecnológicos que asegure la continuidad de los sistemas de información que considere indispensables.
b) La OITEC debe asegurar que los componentes redundantes operan ante la ausencia o caída de los componentes principales.
c) La OITEC debe asegurar la disponibilidad de copias de respaldo de información de servidores y la efectividad de su restauración en casos de recuperación de información.

8.13. Sobre el cumplimiento

El PRONABEC busca prevenir el incumplimiento de las obligaciones legales, reglamentarias o contractuales relativas a la seguridad de la información y así garantizar una gestión de la seguridad de la información en concordancia con la Directiva de Seguridad de la Información del PRONABEC.

8.13.1. Cumplimiento de los requisitos legales y contractuales

Obligaciones:

a) El PRONABEC debe establecer los términos, condiciones y finalidades para la protección de datos personales en cumplimiento con la Ley vigente.

b) La OITEC debe garantizar el uso de software legal que no atente contra los derechos de propiedad intelectual (software pirata, ilegal).
c) La OITEC debe implementar mecanismos para obtener el consentimiento para el tratamiento de datos personales con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar o transmitir dichos datos personales, en el marco de las actividades de la entidad.
d) El PRONABEC tiene los derechos de propiedad intelectual sobre todos los sistemas, aplicativos, manuales, y documentos físicos como digitalizados, desarrollados tanto por personal interno (de cualquier régimen laboral) como por personal externo (proveedores de servicios) que se encuentra en el dominio de la entidad.

8.13.2. Revisión independiente de la seguridad de la información

Obligaciones:

a) La OITEC debe realizar la supervisión del cumplimiento de procedimientos y políticas relacionadas con la Seguridad Informática y de la Seguridad de la Información que se implemente o estén implementados.
b) La OITEC debe planificar la pertinencia de auditorías periódicas internas y externas de seguridad de la información y con auditores independiente al proceso a auditar.

9. RESPONSABILIDADES

La Directiva de Seguridad de la Información es de cumplimiento obligatorio para todo el personal del PRONABEC, incluyendo a personas bajo contratos de locación y proveedores que prestan servicios al PRONABEC ya sean del sector público o privado, cuyas obligaciones deberán estar consignadas en los acuerdos de confidencialidad que suscriban.

El incumplimiento de la presente Directiva dará lugar a la aplicación de medidas administrativas disciplinarias conforme a las disposiciones señaladas en los documentos normativos de la Entidad, sin perjuicio de la responsabilidad civil y/o penal a que hubiere lugar.

A continuación, se señalan los derechos, obligaciones o prohibiciones de los actores:

9.1. Sobre el personal del PRONABEC

9.1.1. Derechos

a) Participar en la implementación y cumplimiento de las disposiciones de seguridad de la información, planes de continuidad, acciones de tratamiento de riesgos y acciones correctivas de acuerdo al alcance de sus funciones.
b) Solicitar la asistencia técnica a la OITEC para la habilitación o configuración de los equipos informáticos y software para su adecuado uso.
c) Reportar o notificar a la OITEC cuando se tenga sospecha de que su contraseña es conocida por otra persona o de algún otro indicio de vulnerabilidad.

9.1.2. Obligaciones

a) Proteger la información que se encuentre en las diferentes unidades de almacenamiento (físico y digital) y que esté bajo su administración o permiso de uso, aun cuando no se utilice y contenga información CONFIDENCIAL o RESERVADA.
b) Utilizar exclusivamente los servicios e infraestructura institucional para todo flujo y trasmisión de información de propiedad del PRONABEC.
c) Utilizar los activos de información que le sean asignados sólo y exclusivamente para fines de sus funciones y actividades laborales, debiendo cumplir con los procedimientos formales de tratamiento e intercambio de información.

d) Mantener la confidencialidad de las credenciales de acceso otorgadas y usarlas diligentemente, asumiendo la responsabilidad por las acciones que terceras personas puedan realizar.
e) Realizar el cambio de su contraseña de acuerdo a la periodicidad establecida.
f) Utilizar contraseñas seguras de acuerdo a todas las recomendaciones establecidas.
g) Utilizar el software antivirus para el escaneo de software malicioso en los diferentes medios de almacenamiento interno o externo del equipo de cómputo.
h) Bloquear su equipo de cómputo cuando se ausente de su lugar de trabajo, así como guardar en una ubicación segura sus documentos, medios magnético u óptico.
i) Velar para que los archivos descargados provenientes de adjuntos de los correos electrónicos, páginas web de internet o copiados de cualquier medio de almacenamiento, provengan de fuentes conocidas y seguras para evitar el riesgo de contagio de virus informáticos y/o instalación de software malicioso en el equipo de cómputo.
j) Identificar, organizar y clasificar su información crítica para que pueda ser almacenada y respaldada bajo el servicio de almacenamiento en nube del PRONABEC.
k) Dejar toda información asignada bajo custodia al jefe inmediato o al que éste designe en caso de ausencia por vacaciones o licencias (> a 30 días) conforme a los procedimientos establecidos en las “Normas para la Entrega y recepción de Cargo del personal del PRONABEC” aprobado mediante Resolución Directoral Ejecutiva N° 283-2019-MINEDU/VMGI-PRONABEC, que garantizan una adecuada trasferencia de funciones y continuidad de servicios en las distintas oficinas y unidades del PRONABEC.
l) Comunicar a su jefe inmediato en caso de evidenciar (ser testigo) una acción o evento que transgreda o que contravengan la presente directiva.

9.1.3. Prohibiciones

a) Está prohibido el uso de información personal o fácilmente deducible como contraseña.
b) Está prohibido que las contraseñas se encuentren en forma legible en cualquier medio impreso, así como dejarlos en lugares visibles o remitirlas por correo electrónico.
c) Está prohibido almacenar las contraseñas en aplicativos, programas o sistemas que proporcionen esta facilidad.
d) Está prohibida la inhabilitación, eliminación o cambio de la configuración del software de antivirus establecida por el PRONABEC.
e) Está prohibido el envío de cadenas de mensajes (spam) con contenido comercial, político, religioso, discriminatorio y demás contenido que degraden la condición humana y resulte ofensivas.
f) Está prohibido el reenvío de correos electrónicos institucionales que contengan información CONFIDENCIAL o RESERVADA hacia otros correos electrónicos que no sean del PRONABEC, salvo autorización de su jefe inmediato o quien asuma sus funciones durante su ausencia.
g) Está prohibido el uso de servicios de correo electrónico y servidores de almacenamiento no institucionales como los servicios gratuitos de Google, Hotmail, etc. para el intercambio y trasmisión de información del PRONABEC.
h) Está prohibido abrir correos electrónicos de remitentes desconocidos o con archivos adjuntos con contenido dudoso más aún si estos han sido identificados como correo no deseado o Spam.
i) Está prohibido suscribir la cuenta de correo electrónico institucional en grupos, listas de interés o catálogos para recibir ofertas de productos o para recibir publicidad o información que no esté relacionada a las labores institucionales.
j) Está prohibido el traslado físico de bienes y/o activos sin la autorización de su jefe inmediato y la OAF.

k) Está prohibido el uso de herramientas informáticas (hardware y software) para vulnerar los controles de seguridad informática, salvo previa autorización, planificación y supervisión de la OITEC.
l) Está prohibido escribir, generar, copiar, coleccionar, propagar, ejecutar o introducir cualquier tipo de código (programas maliciosos), desarrollados para auto replicar, dañar o afectar el funcionamiento o acceso a los equipos de cómputo, redes o información del PRONABEC.

9.2. Sobre los Directores de Oficina y de Unidad

9.2.1. Derechos

a) Difundir las leyes, normas y reglamentos que regulen los temas sobre seguridad de la información, protección de datos personales y otras que salvaguarden los activos de información institucional.
b) Designar y autorizar los permisos y privilegios de acceso para todo el personal a cargo, que accederá a los sistemas de información y plataformas informáticas.
c) Delegar la gestión de accesos y nombrar administradores de sistemas de información siempre que esta característica esté disponible.
d) Reportar las posibles brechas, incidentes y deficiencias en materia de seguridad de la información dentro de su ámbito de gobernanza, funciones y competencias.

9.2.2. Obligaciones

a) Cumplir con la presente directiva y coadyuvar en la implementación del Sistema de Seguridad de la Información, garantizando la confidencialidad, disponibilidad e integridad de su información.
b) Hacer cumplir las disposiciones de seguridad de la información al interior de cada órgano, unidad orgánica o área a su cargo, en el ámbito funcional, técnico y administrativo, según corresponda.
c) Garantizar la confidencialidad de la información bajo su competencia, comprobando que las normas y reglamentos se cumplan.
d) Inscribir los bancos de datos (digitales e impresos bajo su responsabilidad) en cumplimiento de la Ley de Protección de Datos Personales.
e) Solicitar autorización a la Unidad de Abastecimiento de la OAF para la movilización o traslado físico de bienes a otra ubicación.
f) Gestionar la solicitud de grupos de colaboración, listas de distribución, buzones compartidos, cuentas de acceso para locadores y proveedores de acuerdo a las necesidades de su oficina ante la OITEC.
g) Asegurar la incorporación de las consideraciones de seguridad de la información (organizativos, jurídicos y técnicos) asociados a la transferencia y/o acceso de información en los requerimientos de bienes y servicios.
h) Asegurar que todo proveedor de servicio (directo y subcontratado) que trate información del PRONABEC, conozca las políticas y procedimientos de seguridad que le sean aplicables y que suscriba un acuerdo de confidencialidad y de no divulgación.

9.3. Sobre el Oficial de Seguridad de la Información

9.3.1. Obligaciones

a) Revisar y evaluar anualmente las políticas, objetivos, planes, normas, directivas, responsabilidades asociadas a la seguridad de la información para su adecuación a la normatividad vigente.

b) Proponer al CGD las directivas, políticas, objetivos, planes, roles, funciones y modificaciones necesarias para gestionar de manera eficiente y efectiva la seguridad de la información, para su aprobación por el titular del PRONABEC.
c) Coordinar, establecer y aplicar una metodología de gestión de riesgos.
d) Auditar y evaluar el cumplimiento de los controles y las prácticas de seguridad de la información; debiendo comunicar al CGD de las faltas e infracciones al cumplimiento del contenido de las disposiciones establecidas.
e) Identificar las necesidades de capacitación, difusión y sensibilización en seguridad de la información.
f) Informar continuamente al personal del PRONABEC acerca de los objetivos, medidas y reglamentaciones en materia de seguridad de la información que se encuentren en vigencia.
g) Evaluar los eventos reportados para actualizar la clasificación de los incidentes de seguridad de la información, evaluando la causa, probabilidad e impacto.
h) Gestionar las acciones requeridas para desarrollar el análisis a profundidad de los incidentes reportados pudiendo solicitar la ejecución de técnicas más complejas como la informática forense, mediante un peritaje informático, de corresponder.
i) Reportar los incidentes de seguridad de la información al Centro Nacional de Seguridad Digital de la Secretaría de Gobierno Digital, en su calidad de ente rector en gobernanza de datos.
j) Reportar el estado de implementación del SGSI a la Secretaría de Gobierno Digital, en su calidad de ente rector en gobernanza de datos.
k) Establecer contacto con grupos especializados en seguridad de la información y ciberseguridad a fin de garantizar el aprendizaje y la mejora continua del SGSI.

9.4. Sobre el personal bajo contrato de locación y proveedores

9.4.1. Obligaciones

a) Utilizar los activos de información que le sean asignados sólo y exclusivamente para fines de las actividades establecidas según contrato, debiendo cumplir con los procedimientos formales de tratamiento e intercambio de información.
b) Mantener la confidencialidad de las credenciales de acceso otorgadas y usarlas diligentemente, asumiendo la responsabilidad por las acciones que terceras personas puedan realizar.
c) Atender a lo establecido en la sección “8.10 Sobre las relaciones con los proveedores” del presente documento.

9.5. Sobre el personal de seguridad física:

9.5.1. Funciones

a) Realizar el registro respectivo de cajas, bolsas, paquetes, maletines, carteras y otros que porten los ciudadanos/as en condición de visitante, antes del ingreso y salida de las instalaciones del PRONABEC.
b) Realizar la supervisión de seguridad correspondiente a fin de mantener asegurado el perímetro de las instalaciones.
c) Asegurar que todo personal visitante cuente con la autorización para el ingreso de las instalaciones y áreas restringidas de ser el caso.
d) Controlar el ingreso con armas punzo cortantes y/o penetrantes y armas de fuego, en caso de presentarse, debe ser registrado y dejado en custodia en el puesto de seguridad del Edificio. Están exceptuados el propio personal de seguridad del PRONABEC.

9.5.2. Obligaciones

a) Registrar todas las visitas en el Registro de Visitas, conforme lo dispuesto en la R.M. N° 035-2017 PCM y la normativa vigente.