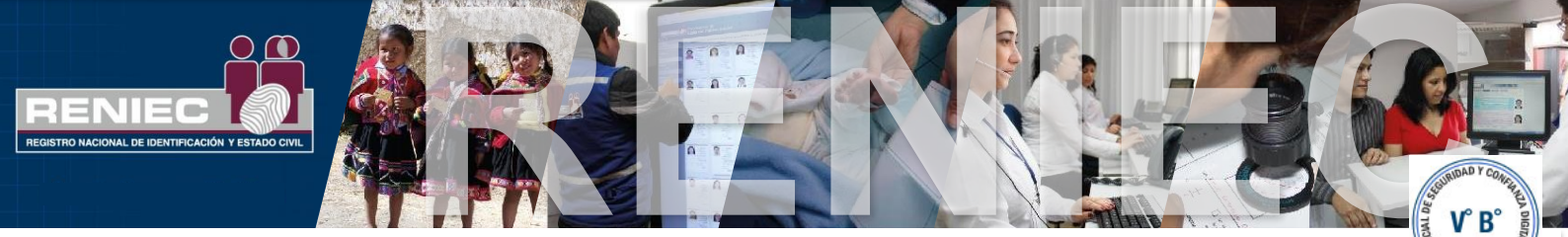

DIRECTIVA

DI-036-SGEN/003

CONTROLES FÍSICOS DE SEGURIDAD DE LA INFORMACIÓN DEL SGSI - RENIEC

PRIMERA VERSIÓN

SECRETARÍA GENERAL

ÍNDICE

I. OBJETIVO

Establecer los lineamientos que orienten a gestionar los controles físicos de Seguridad de la Información, que permitan proteger la confidencialidad, integridad y disponibilidad de la información y de los sistemas que soportan a los procesos del Registro Nacional de Identificación y Estado Civil RENIEC, bajo la norma ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos.

II. ALCANCE

La presente Directiva es administrada por la Secretaría General, y es de aplicación obligatoria para todos los órganos y unidades orgánicas que conforman el RENIEC.

III. BASE LEGAL

3.1. **Ley N° 26497**, Ley Orgánica del Registro Nacional de Identificación y Estado Civil, del 12 julio de 1995 y sus modificatorias.

3.2. **Ley Nº 27269**, Ley de Firmas y Certificados Digitales, del 28 de mayo de 2000 y su modificatoria.

3.3. **Ley N° 27309,** Ley que incorpora los delitos informáticos al Código Penal, del 17 de julio de 2000.

3.4. **Ley N° 27658,** Ley Marco de Modernización de la Gestión del Estado, del 30 de enero de 2002 y sus modificatorias.

3.5. **Ley N° 28716**, Ley de Control Interno de las Entidades del Estado, del 18 de abril de 2006 y sus modificatorias.

3.6. **Ley N° 29733**, Ley de Protección de Datos Personales, del 3 de julio de 2011 y sus modificatorias.

3.7. **Decreto de Urgencia N° 006-2020**, que crea el Sistema Nacional de Transformación Digital, del 9 de enero de 2020.

3.8. **Decreto de Urgencia N° 007-2020**, que aprueba el Marco de Confianza Digital, del 9 de enero de 2020.

3.9. **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, del 7 de enero de 2017 y sus modificatorias.

3.10. **Decreto Legislativo N° 1412**, que aprueba la Ley de Gobierno Digital, del 13 de setiembre de 2018.

3.11. **Decreto Supremo N° 030-2002-PCM**, que aprueba el Reglamento de la Ley Marco de Modernización de la Gestión del Estado, del 3 de mayo de 2002.

3.12. **Decreto Supremo N° 072-2003-PCM**, que aprueba el Reglamento de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, del 7 de agosto de 2003.

3.13. **Decreto Supremo N° 052-2008-PCM**, que aprueba el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales, del 19 de julio de 2008 y sus modificatorias.

3.14. **Decreto Supremo N° 003-2013-JUS**, que aprueba el Reglamento de la Ley de Protección de Datos Personales, del 22 de marzo de 2013.

3.15. **Decreto Supremo N° 019-2017-JUS**, que aprueba el Reglamento del Decreto Legislativo N° 1353, Decreto Legislativo 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, del 15 setiembre de 2017, y sus modificatorias.

3.16. **Decreto Supremo N° 033-2018-PCM**, que crea de la Plataforma Digital Única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital, del 23 de marzo de 2018.

3.17. **Decreto Supremo N° 123-2018-PCM**, que aprueba el Reglamento del Sistema Administrativo de Modernización de la Gestión Pública, del 19 de diciembre de 2018.

3.18. **Decreto Supremo N° 004-2019-JUS**, que aprueba el Texto Único Ordenado de la Ley Nº 27444, Ley del Procedimiento Administrativo General, del 25 de enero de 2019, y sus modificatorias.

3.19. **Decreto Supremo N° 021-2019-JUS**, que aprueba el Texto Único Ordenado de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública, del 11 de diciembre de 2019, y su modificatoria.

3.20. **Decreto Supremo N° 029-2021-PCM**, que aprueba el Reglamento del Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, del 19 de febrero de 2021.

3.21. **Decreto Supremo N° 103-2022-PCM**, que aprueba la Política Nacional de Modernización de la Gestión Pública al 2030, del 21 de agosto de 2022.

3.22. **Resolución Ministerial N° 073-2004-PCM**, que aprueba la "Guía para la Administración Eficiente de Software Legal en la Administración Pública", del 17 de marzo de 2004.

3.23. **Resolución Ministerial N° 087-2019-PCM**, que aprueba las disposiciones sobre la conformación y funciones del Comité de Gobierno Digital, del 19 de marzo de 2019.

3.24. **Resolución de Contraloría Nº 320-2006-CG**, que aprueba las Normas de Control Interno, del 3 de noviembre de 2006.

3.25. **Resolución de Contraloría Nº 146-2019-CG**, que aprueba la Directiva N° 006-2019-CG/INTEG "Implementación del Sistema de Control Interno en las entidades del Estado", del 17 de mayo de 2019 y modificatorias.

3.26. **Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD**, que aprueba la Directiva Nº 001-2023-PCM/SGTD, Directiva que establece el perfil y responsabilidades del Oficial de seguridad y confianza digital, del 8 de setiembre de 2023.

3.27. **Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD**, que establece la implementación y mantenimiento del sistema de gestión de seguridad de la información en las entidades públicas, del 8 de setiembre de 2023.

3.28. **Resolución Directoral N° 022-2022-INACAL/DN**, que aprueba la Norma Técnica Peruana NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición. Reemplaza a la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, del 12 de enero de 2023.

3.29. **Resolución Jefatural Nº 000176-2022/JNAC/RENIEC**, que aprueba la conformación del Equipo de Respuestas ante Incidentes en Seguridad Digital del Registro Nacional de Identificación y Estado Civil, del 12 de octubre de 2022.

3.30. **Resolución Jefatural N° 000153-2023/JNAC/RENIEC**, que aprueba la Política y Objetivos de Seguridad de la Información del Registro Nacional de Identificación y Estado Civil – RENIEC, del 18 de setiembre de 2023.

3.31. **Resolución Jefatural N° 0000185-2023/JNAC/RENIEC**, que resuelve reconformar el Comité de Gobierno Digital del Registro Nacional de Identificación y Estado Civil – RENIEC, constituido mediante Resolución Jefatural N° 000107-2019/JNAC/RENIEC (22JUL2019) y reconformado por Resolución Jefatural N° 000156-2019/JNAC/RENIEC (26SET2019) y Resolución Jefatural N° 000183-2020/JNAC/RENIEC (17NOV2020) y Resolución Jefatural N°022-2022/JNAC/RENIEC (14FEB2022), y modificado mediante la Resolución Jefatural N°0147-2023/JNAC/RENIEC (01SET2023), del 21 de noviembre de 2023.

3.32. **Resolución Jefatural Nº 000061-2024/JNAC/RENIEC**, aprueba el Reglamento de Organización y Funciones y la Estructura Orgánica del Registro Nacional de Identificación y Estado Civil - RENIEC, del 08 de abril de 2024.

3.33. **Resolución Jefatural N° 000067-2024/JNAC/RENIEC,** aprueba el Cuadro de Equivalencias y Siglas de las unidades de organización del RENIEC, del 22 de abril de 2024.

3.34. **Resolución Secretarial Nº 000084-2024/SGEN/RENIEC**, que aprueba la Directiva DI-001-OPPM/001 “Documentos Normativos del RENIEC”, del 08 de julio de 2024.

3.35. **Norma Internacional ISO 27001:2022** Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos; publicada el 25 octubre de 2022.

3.36. **Norma Internacional ISO 27002:2022** Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información; publicada el 29 de diciembre de 2022.

IV. TÉRMINOS Y DEFINICIONES

4.1. Abreviaciones/siglas

En la presente directiva se utilizan las siguientes abreviaciones/siglas:

SIGLAS DE LAS UNIDADES DE ORGANIZACIÓN DEL RENIEC	
JNAC	Jefatura Nacional
GG	Gerencia General
SGEN	Secretaría General
OSDN	Oficina de Seguridad y Defensa Nacional
OTI	Oficina de Tecnologías de la Información
UIST	Unidad de Infraestructura y Soporte Tecnológico
OAF	Oficina de Administración y Finanzas

USGCP	Unidad de Servicios Generales y Control Patrimonial
RENIEC	Registro Nacional de Identificación y Estado Civil

Referencia: Cuadro de Equivalencias y Siglas de los órganos y unidades orgánicas del RENIEC – Resolución Jefatural N° 000067-2024/JNAC/RENIEC, de fecha 22 de abril del 2024.

ABREVIATURA	NOMBRE
EREP	Entidad de Registro del Estado Peruano
ISO	International Organization for Standardization (Organización Internacional de Estandarización)
SGSI	Sistema de Gestión de la Seguridad de la Información
OSCD	Oficial de Seguridad y Confianza Digital

4.2. Activo de Información

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, entre otros) que tenga valor para la organización.

4.3. Ciberseguridad

Capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país.

4.4. Confianza Digital

Es el estado que emerge como resultado de cuán veraces, predecibles, éticas, proactivas, transparentes, seguras, inclusivas y confiables son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital, con el propósito de impulsar el desarrollo de la economía digital y la transformación digital. Es un componente de la transformación digital y tiene como ámbitos la protección de datos personales, la ética, la transparencia, la seguridad digital y la protección del consumidor en el entorno digital.

4.5. Confidencialidad

Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

4.6. Clasificación

Es el acto de disponer con carácter público, confidencial, reservado y secreto de la información mediante acto resolutivo.

4.7. Desclasificación

Es el acto de disponer con carácter público la información declarada con carácter secreto, reservado o confidencial mediante acto resolutivo.

4.8. Disponibilidad

Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

4.9. Dueño del proceso
Es quien tiene la responsabilidad y autoridad para participar en el proceso de gestión de riesgos de seguridad de la información.

- Los dueños de procesos a cargo de las unidades de organización de la entidad son responsables de apoyar en la gestión de riesgos e implementación de los controles de seguridad de la información identificados en sus ámbitos de competencia, así como también coadyuvan en la gestión de incidentes según corresponda[1].

4.10. Evento
Ocurrencia o cambio de un conjunto particular de circunstancias.

4.11. Incidente de Seguridad de la Información
Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

4.12. Incidente de seguridad digital
Evento o serie de eventos que pueden comprometer la confianza, la prosperidad económica, la protección de las personas y sus datos personales, la información, entre otros activos de la organización, a través de tecnologías digitales.

4.13. Información
La información es un activo que, al igual que otros activos importantes, es esencial para una organización y en consecuencia debe ser protegido adecuadamente. La información puede ser almacenada de muchas formas, incluyendo: forma digital (por ejemplo, en archivos de datos almacenados en medios electrónicos u ópticos), forma material (por ejemplo, en papel), así como información de conocimiento técnico de los servidores.

4.14. Riesgo
Probabilidad que una amenaza se materialice, al producirse exposición a una vulnerabilidad existente.

4.15. Sistema de Gestión de Seguridad de la Información
Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque a procesos, gestión del riesgo y de mejora continua.

4.16. Servidores Civiles
Toda persona que tiene un vínculo laboral o contrato administrativo de servicio con el Estado. Son los usuarios internos del RENIEC

V. RESPONSABILIDADES
En función de los controles físicos de seguridad de la información del SGSI, se establecen las responsabilidades de los Dueños del Proceso/s, órganos y unidades

[1] Inciso 4.8 del Artículo 4. Responsables en la gestión de la seguridad digital institucional de la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD.

orgánicas involucradas[2].

5.1. Jefatura Nacional JNAC

Es responsable de la implementación del SGSI, para lo cual, como mínimo, debe aprobar las políticas y objetivos para implementar, operar, mantener y mejorar el SGSI.

5.2. Secretaría General SGEN

Es la encargada de informar semestralmente al Titular de la entidad los avances y dificultades en la implementación u operación del SGSI, así como el cumplimiento de la presente Resolución.

Asimismo, es responsable de asegurar el cumplimiento de las políticas, objetivos, planes, procedimientos y marco normativo en materia de seguridad y confianza digital en la entidad pública.

5.3. Comité de Gobierno y Transformación Digital

Es responsable de la dirección, mantenimiento y supervisión estratégica de los planes, resultados y recursos del SGSI. Asimismo, a solicitud del Titular de la entidad o la máxima autoridad administrativa emite opinión y recomendaciones sobre la gestión estratégica del SGSI[3]. Sin perjuicio de lo indicado la entidad puede solicitar opinión a un órgano consultivo vinculado a la gestión de riesgos de la entidad.

5.4. Dueños del Proceso, Órganos y Unidades Orgánicas del RENIEC

Los Dueños del Proceso, Órganos y Unidades Orgánicas del RENIEC, son responsables de cumplir con las disposiciones emanadas en la presente Directiva; según lo descrito en el sub numeral 6.1 y detallado en el título VII. Disposiciones Específicas los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente. Así como de la difusión y despliegue de las disposiciones normativas a todos los servidores bajo su cargo.

5.5. Oficina de Seguridad y Defensa Nacional OSDN

Es responsabilidad de la OSDN, en coordinación con la OTI/UIST, velar por el cumplimiento de los controles físicos de seguridad de la información según lo descrito en el sub numeral 6.2 y detallado en el título VII. Disposiciones Específicas los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.

5.6. Oficina de Tecnología de la Información OTI

Es responsabilidad de la OTI, a través de la Unidad de Infraestructura y Soporte Tecnológico UIST, en coordinación con la OSDN, velar por el cumplimiento de los controles físicos de seguridad de la información según lo descrito en el sub numeral 6.3 y detallado en el título VII. Disposiciones Específicas los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.

5.7. Oficina de Administración y Finanzas OAF

Es responsabilidad de la OAF a través de la Unidad de Servicios Generales y Control Patrimonial USGCP, normar en concordancia con los procesos y procedimientos establecidos por la Dirección General de Abastecimiento, los

[2] Los controles de seguridad de la información, son identificados en la Tabla A.1 Controles de Seguridad de la Información, numeral 7. Controles Físicos, de la norma NTP - ISO/IEC 27001:2022 Seguridad de la Información, Ciberseguridad y Protección de la Privacidad. Sistemas de Gestión de Seguridad de la Información. Requisitos.

[3] Inciso 4.3 del Artículo 4. Responsables en la gestión de la seguridad digital institucional de la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD.

documentos normativos del RENIEC pertinentes; así como, los relacionados a la salida e ingreso de bienes muebles patrimoniales de carácter informático por cualquier modalidad y/o motivo, según lo descrito en el sub numeral 6.4 y detallado en el título VII. Disposiciones Específicas que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.

5.8. Oficial de Seguridad y Confianza Digital OSCD, es responsable de:

5.8.1 Coordinar la implementación, operación, mantenimiento y mejora continua del SGSI del RENIEC[4].

5.8.2 Coordinar con las unidades de organización de la entidad las acciones orientadas a implementar y/o mantener el SGSI del RENIEC.

5.8.3 Formular y actualizar la presente Directiva y procedimientos en materia de Seguridad de la Información acorde a lo dispuesto en la Directiva DI-001-OPPM/001 "Documentos Normativos del RENIEC".

5.8.4 Coordinar con el Líder de Gobierno y Transformación Digital, lo concerniente a iniciativas y proyectos en materia de seguridad y confianza digital.

5.8.5 Informar a la máxima autoridad administrativa acerca de los avances y dificultades en la implementación u operación del SGSI del RENIEC; así como resultados de las auditorías de seguridad de la información internas y/o externas realizadas anualmente a la entidad, y sobre la aplicación efectiva de las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.

VI. DISPOSICIONES GENERALES

6.1. Los Dueños del Proceso, Órganos y Unidades Orgánicas del RENIEC, conforme a sus funciones cuentan con facultades para definir o actualizar los controles físicos de seguridad de la información contenidos en la presente Directiva, en coordinación con la OSCD, OSDN, OTI/UIST y OAF/USGCP.

6.2. La OSDN gestiona los controles relacionados a perímetros de seguridad física, ingreso físico, asegurar oficinas, salas e instalaciones, supervisión de la seguridad física, protección contra amenazas físicas y ambientales, trabajos en áreas seguras, servicio de suministro de apoyo, seguridad de cableado y mantenimiento de equipos.

6.3. La OTI/UIST gestiona los controles relacionados al trabajo en áreas seguras, escritorio y pantalla limpia, ubicación y protección de datos, seguridad de los activos fuera de las instalaciones, medios de almacenamiento, servicios de suministro de apoyo, seguridad del cableado, mantenimiento de equipos y eliminación segura o reutilización de equipos.

6.4. La OAF/USGCP gestiona los controles relacionados a ubicación y protección de los equipos, seguridad de los activos fuera de las instalaciones, servicios de suministro de apoyo y seguridad del cableado.

VII. DISPOSICIONES ESPECÍFICAS

Los controles físicos de la seguridad de la información son transversales a los procesos de la institución y han sido desarrollados en cumplimiento de los

[4] Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD

requisitos del Anexo A Tabla A.1 Controles de seguridad de la información de la NTP - ISO 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos.

7.1. Controles físicos (ISO 27001 A.7)

7.1.1. Perímetros de seguridad física (ISO 27001 A.7.1)

7.1.1.1. La OSDN, establece lineamientos para evitar el acceso físico no autorizado, con consecuencia de daño y la posible fuga de la información, así como, proporcionar seguridad a los perímetros de las sedes del RENIEC, debe evaluar y recomendar lo siguiente:

a. Las características de las instalaciones de perímetros físicamente seguros para funcionamiento de oficinas de procesamiento de la información con puertas y accesos adecuadamente protegidos contra accesos no autorizado. Las diferentes oficinas registrales y locales verificarán que las puertas y ventanas deben asegurarse cuando estén desatendidas y considerar la protección externa para las ventanas, efectuando el requerimiento al área correspondiente ubicadas en primer piso o de fácil acceso, también considerar los puntos de ventilación por riesgo de intrusión.

b. Las características técnicas de las puertas corta fuego cuando sea necesario, que permita el efectivo flujo a la salida y restrinja el acceso no autorizado de ser el caso.

c. Las barreras físicas alrededor de las instalaciones o sedes del RENIEC para controlar o restringir el acceso físico no autorizado y fortalecer las barreras en condiciones de mayor amenaza o exposición.

7.1.1.2. La OSDN, define los controles físicos y otras medidas de seguridad de su competencia en el RENIEC, en la Directiva DI-206-OSDN/001 "Seguridad de las instalaciones en sedes, oficinas registrales, agencias, locales y/o puntos de atención"; la Guía de procedimiento GP-266-OSDN/002 "Sistema de Video Vigilancia CCTV digital - IP en sedes y oficinas registrales del área de Lima y Callao" y la NAI-386-OSDN/005 "Normas y obligaciones del personal de vigilancia privada".

7.1.2. Ingreso físico (ISO 27001 A.7.2)

7.1.2.1. La OSDN, establece los lineamientos del acceso físico y otras medidas de seguridad del RENIEC en la Directiva DI-206-OSDN/001 "Seguridad de las instalaciones en sedes, oficinas registrales, agencias, locales y/o puntos de atención"; la Guía de Procedimiento GP-325-OSDN/003 "Control de visitas en las sedes administrativas, operativa, Registros Civiles y Jirón Ancash"; la Guía de Procedimiento GP-344-OSDN/004 "Ingreso de contratistas, visitantes y personal del RENIEC en días y horarios no laborables, a las instalaciones del RENIEC", la NAI-386-OSDN/005 "Normas y obligaciones del personal de vigilancia privada" y la NAI-376-OSDN/004 "Diseño,

elaboración y control del pase provisional de identificación (fotocheck provisional) y pase de visita".

7.1.2.2. En el caso de personas no autorizadas, el ingreso a las instalaciones del RENIEC debe ser controlada, bajo las siguientes condiciones:

a. Limitar el acceso a las instalaciones del RENIEC solo al personal autorizado a excepción de las áreas de atención a los ciudadanos

b. Mantener el registro físico del acceso a las sedes, además del control de ingreso y salida de equipos a cargo de los órganos y unidades orgánicas en coordinación con la OSDN.

c. Recomendar la implementación de procesos y mecanismos técnicos para la gestión del acceso a las áreas donde se procesa o almacena la información (uso de tarjetas de acceso, biometría o autenticación de dos factores).

d. Establecer un área de recepción monitoreada por personal u otros medios para controlar el acceso físico al sitio o edificio.

e. Revisar los efectos personales (bolsas, maletines, paquetes) del personal y visitas, durante la entrada y salida de las instalaciones.

f. Uso obligatorio de fotochek, pases de visita u otros para identificar a los empleados permanentes, proveedores y visitantes, durante su permanencia en las instalaciones.

g. Verificar el acceso a proveedores a las áreas seguras o instalaciones de procesamiento de información solo cuando sea necesario.

7.1.2.3. En el caso de visitantes:

a. Cursar comunicación por el Centro de Control y Monitoreo, Jefes de oficina y locales.

b. Registrar, destino, lugar donde se dirige, fecha y hora de ingreso y salida.

c. Permitir acceso solo para fines específicos, autorizados y con instrucciones sobre los requisitos de seguridad del área y procedimientos de emergencia.

d. Verificar el acceso de visitantes o contratistas solicitadas por el área usuaria, técnica o especializada, hasta el lugar de destino, salvo que se conceda una excepción explicita.

7.1.2.4. Para el caso de zonas de entrega y recepción de material, el órgano y unidad orgánica usuaria debe:

a. Registrar la entrega y/o recepción de acuerdo con los procedimientos de gestión de activos.

b. Inspeccionar la recepción de los materiales en busca de evidencias de manipulación. Si se evidencia una

manipulación, se debe comunicar de inmediato al personal de seguridad.

c. Identificar, inspeccionar y controlar los materiales y/o activos considerados como materiales peligrosos afín de controlar su manipulación y acopio correcto en áreas de salida, recepción y carga.

d. Separar físicamente los envíos entrantes y salientes, cuando sea posible.

7.1.3. Asegurar oficinas, salas e instalaciones (ISO 27001 A.7.3)

7.1.3.1. La OSDN, evalúa y recomienda los lineamientos para asegurar oficinas, salas e instalaciones, para prevenir el acceso físico no autorizado, el daño y a posible fuga de la información; teniendo en cuenta lo siguiente:

a. La ubicación de las instalaciones críticas en cada sede o local para evitar el acceso no autorizado además del rotulado o señalización que corresponda por el área usuaria.

b. El acondicionamiento de las instalaciones por el área usuaria para evitar que la información o actividades confidenciales sean visibles y audibles desde el exterior.

7.1.3.2. La OSDN, define los lineamientos para asegurar las oficinas, las salas y las instalaciones y otras medidas de seguridad del RENIEC, en la Directiva DI-206-OSDN/001 "Seguridad de las instalaciones en sedes, oficinas registrales, agencias, locales y/o puntos de atención" y en la NAI-386-OSDN/005 "Normas y obligaciones del personal de vigilancia privada".

7.1.3.3. Cuando las instalaciones de las oficinas del RENIEC, se encuentren vacías, se deben apagar las luces a fin de contribuir positivamente con acciones para disminuir los efectos del cambio climático.

7.1.4. Supervisión de la seguridad física (ISO 27001 A.7.4)

La OSDN:

7.1.4.1. Diseña, recomienda y monitorea los sistemas de video vigilancia que permite la vigilancia visual en las sedes y oficinas registrales del RENIEC del área de Lima y Callao, así como en las oficinas principales de provincias.

7.1.4.2. Establece los lineamientos para la vigilancia de la seguridad física del RENIEC, en la Directiva DI-206-OSDN/001 "Seguridad de las instalaciones en sedes, oficinas registrales, agencias, locales y/o puntos de atención" y en la NAI-386-OSDN/005 "Normas y obligaciones del personal de vigilancia privada".

7.1.4.3. Supervisa y controla la seguridad física de las instalaciones y locales del RENIEC, mediante una empresa de seguridad y vigilancia, quienes cumplen sus funciones de vigilancia con consignas, entre otras, de temas de seguridad física.

7.1.4.4. Monitorea continuamente el acceso a las oficinas donde se procesa información, con el objetivo de detectar accesos no autorizados o comportamientos sospechosos, mediante sistemas de video vigilancia, y se registra los accesos a las áreas consideradas sensibles.

7.1.5. Protección contra amenazas físicas y ambientales (ISO 27001 A.7.5)

La OSDN:

7.1.5.1. Formula e implementa planes para la protección contra amenazas físicas y ambientales, como fenómenos naturales, amenazas físicas intencionales o no intencionales a la infraestructura, como: incendios, inundaciones, terremotos, explosiones, disturbios civiles, desechos tóxicos, emisiones ambientales.

7.1.5.2. Formula los lineamientos para la protección contra las amenazas establecidas en la Directiva DI-206-OSDN/001 "Seguridad de las instalaciones en sedes, oficinas registrales, agencias, locales y/o puntos de atención", la NAI-386-OSDN/005 "Normas y obligaciones del personal de vigilancia privada" y la NAI-368-OSDN/003 "Indicaciones a seguir ante señales de alerta del sistema de alarma de incendio y aniego".

7.1.6. Trabajos en áreas seguras (ISO 27001 A.7.6)

7.1.6.1. Las áreas seguras en el RENIEC son aquellas en los que se maneja información sensible y se tiene valiosos equipos informáticos, con los que se alcanzan los objetivos de la organización, por lo tanto, requieren protección contra daños y accesos no autorizados.

7.1.6.2. La OSDN, establece medidas de seguridad aplicables a todo el personal considerando, entre otras, las siguientes pautas:

a. Las áreas usuarias no deben permitir equipos fotográficos, de video, de audio u otros equipos de grabación como cámaras en las áreas seguras o instalaciones de procesamiento de información a menos que se autorice.

b. Publicar protocolos y lineamientos de seguridad, señaléticas, rutas de evacuación (para incendios, movimientos sísmicos, etc.) de manera visible o y accesible.

c. Todo trabajo dentro del área segura es supervisado, por el área usuaria o especializada.

7.1.6.3. Los equipos de comunicación de la OTI/UIST están instalados dentro de gabinetes o cuartos de comunicaciones cerrados con llave y con sistema de alimentación continua de energía en las diferentes Sedes de los centros de atención, Agencias, Oficinas Registrales, Jefatura de Oficinas Regionales, Oficinas Registrales Auxiliares – ORAS y las Oficinas de la Entidad de Registro del Estado Peruano (EREP).

7.1.6.4. Los equipos y servidores de la OTI/UIST están ubicados en los Centros de Cómputo de las sedes principales de la institución (Housing – Santa Catalina y Sede San Borja).

7.1.6.5. Para el acceso de los usuarios al Centro de Cómputo se tienen controles biométricos y tarjeta de aproximación, así como un registro y control foliado, para el control manual de ingresos y salidas, gestionada por la OTI/UIST.

7.1.7. Escritorio y pantalla limpia (ISO 27001 A.7.7)

7.1.7.1. La OTI/UIST, implementa el protector de pantalla institucional, el cual se activa transcurridos cinco minutos de inactividad, en la computadora bloqueando el acceso.

7.1.7.2. El servidor del RENIEC debe cumplir lo siguiente:

a. Bloquear la computadora que utiliza, cuando este se ausente de su puesto de trabajo, presionando simultáneamente las teclas “Control”, “Alt” y “Supr” (o “Del” en algunos casos) y luego seleccionar la opción “Bloquear el equipo”; para evitar el uso no autorizado de un tercero y de las aplicaciones instaladas. El servidor civil que incumpla lo señalado es responsable por el uso no autorizado del equipo, de la red o de las aplicaciones instaladas.

b. Apagar la pantalla de aquellos equipos que no se encuentran en uso, por ejemplo, cuando el personal se encuentra en teletrabajo; a fin de contribuir positivamente con acciones para disminuir los efectos del cambio climático.

c. Mantener los escritorios limpios y libre de hojas y papeles de trabajo con información confidencial o sensible, luego de la jornada laboral. Asimismo, no deben dejar medios de almacenamiento donde se pueda obtener información de la organización. El almacenamiento de estos elementos se debe realizar preferiblemente en gabinetes bajo llave o tener rutas compartidas con el servidor de OTI para el almacenamiento de archivos lógicos.

d. Reducir el uso de papel y reciclar el papel que no contenga información confidencial a fin de contribuir positivamente con acciones para disminuir los efectos del cambio climático.

e. Tener especial cuidado con el uso de dispositivos como fotocopias e impresoras de manera que el material con información confidencial no permanezca en ellas sin atención.

7.1.8. Ubicación y protección de los equipos (ISO 27001 A.7.8)

7.1.8.1. Los recursos informáticos y de comunicaciones que se encuentran en el Centro de Cómputo cuentan con medidas de seguridad tales como: servicio de alimentación de energía eléctrica ininterrumpida, flujo de alimentación de energía eléctrica estabilizada, sistema de refrigeración, control de acceso físico y/o biométrico para el ingreso de los servidores civiles y/o proveedores autorizados.

7.1.8.2. Para el ingreso al Centro de Cómputo se tienen tres tipos de accesos:

a. **Directo**: Se otorga al servidor civil que por naturaleza de sus funciones tiene acceso permanente a las instalaciones del Centro de Cómputo y no requiere autorización expresa. Ejemplo: los operadores de la OTI/UIST.

b. **Autorizado**: Se otorga al servidor civil que requiere ingresar al Centro de Cómputo eventualmente, el cual figura en una lista autorizada, debiéndose registrarse en la bitácora de control de acceso del Centro de Cómputo.

c. **Especial**: Se otorga excepcionalmente al servidor civil o terceros que no figura en la lista autorizada y por lo tanto requiere autorización expresa del responsable del Centro de Cómputo. A su vez debe registrar su ingreso en la bitácora de control de acceso del Centro de Cómputo.

7.1.8.3. La OTI/UIST, es responsable de lo siguiente:

a. Llevar un registro, en concordancia con los registros de la OAF/USGCP, de los bienes muebles patrimoniales de naturaleza informática, los cuales se encuentran registrados en el sistema de administración patrimonial pertinente (SIGA). El traslado de los equipos de comunicaciones se debe realizar en coordinación con la OAF/USGCP, a efecto de que el mismo cuente con las actas de desplazamiento pertinente y la autorización de la OTI/UIST, quien evalúa los riesgos, aprueba y coordina las acciones a realizar para garantizar el normal funcionamiento de los equipos de comunicaciones.

b. Monitorear la temperatura y humedad con el objeto de asegurar las condiciones que permitan el normal desarrollo en instalaciones de procesamiento de información, ya sea para servidores o equipos de cómputo.

7.1.8.4. El administrador de cada Centro de atención, Agencia, Oficina Registral y Oficina de la EREP es responsable por la integridad física de los equipos informáticos y de comunicación a su cargo. Se prohíbe la instalación y manipulación de equipos sin autorización de la OTI.

7.1.8.5. El Operador del Centro de Cómputo es el encargado de registrar, supervisar, custodiar y asistir al visitante. En él recae la responsabilidad del actuar del visitante dentro del área en mención. La presencia de un operador en el Centro de Cómputo debe ser permanente para el monitoreo de la infraestructura TI y facilities (UPS, aire acondicionado, control de accesos, entre otros); a fin de garantizar las actividades de emergencia ante cualquier eventualidad.

7.1.8.6. Los equipos de los servidores civiles deben estar ubicados de forma segura y protegida para reducir los riesgos de amenazas y peligros ambientales y acceso no autorizado.

7.1.8.7. Los equipos de comunicaciones tienen protección tanto física como eléctrica con medios de protección conocidos como gabinete cerrado con llave y sistema de alimentación ininterrumpida.

7.1.8.8. Está prohibido, comer, beber, y fumar en los centros de datos, líneas de producción, archivos, unidades de recepción de documentos, áreas administrativas, entre otros.

7.1.8.9. La OTI/UIST establece normas en relación a los "parámetros de temperatura y humedad relativa en el centro de cómputo", para el monitoreo y el registro diario de la temperatura y humedad relativa en los centros de cómputo del RENIEC.

7.1.9. Seguridad de los activos fuera de las instalaciones (ISO 27001 A.7.9)

7.1.9.1. El responsable del órgano o unidad orgánica debe autorizar la salida de cualquier equipo fuera de las instalaciones del RENIEC que almacena o procese información.

7.1.9.2. El usuario, responsable del activo toma en cuenta todos los riesgos al estar fuera de las instalaciones del RENIEC, tales como el robo o pérdida de dicho activo.

7.1.9.3. La OAF/USGCP define el proceso y los procedimientos para la salida de bienes muebles patrimoniales, los cuales incluyen la generación de las actas y los registros correspondientes, para la salida, desplazamientos internos y/o externos de bienes muebles patrimoniales y/ los que se encuentren bajo administración del RENIEC

7.1.10. Medios de almacenamiento (ISO 27001 A.7.10)

7.1.10.1. La OTI/UIST, establece los siguientes lineamientos a fin de garantizar: la no divulgación, modificación, eliminación o destrucción de la información contenida en los medios de almacenamiento físicos (computadora, laptop, disco duro, entre otros).

a. Los medios de almacenamiento se gestionan a lo largo de su ciclo de vida, desde la adquisición, uso, transporte y desecho de este, de acuerdo con el esquema de clasificación de la información y los requisitos de manipulación.

b. Los medios de almacenamiento deben permanecer en un entorno seguro y protegido de acuerdo con su clasificación de la información que contienen, y deben contar con protección contra amenazas ambientales (calor, humedad, campo electrónico y polvo).

c. Solo se habilitan puertos de almacenamiento extraíbles USB, a solicitud justificada de los responsables de los órganos o unidades orgánicas.

d. En el caso de reutilización de medios de almacenamiento, se deberá realizar el borrado seguro a

fin de minimizar el riesgo de fuga de información, de acuerdo con su clasificación.

7.1.10.2. Para el caso de medios de almacenamiento como el papel, las áreas usuarias deben deshacerse de los mismos, cuando contengan información confidencial, debiendo destruir, triturar o eliminar de forma segura el contenido.

7.1.10.3. Como medida de prevención contra infecciones de malware, fuga y pérdida de la información se restringe el uso de los medios extraíbles de almacenamiento USB, cámaras digitales, módems inalámbricos, unidades de almacenamiento CD/DVD y de dispositivos móviles, para lo cual se definen las siguientes políticas:

a. Para aquellos usuarios que por la naturaleza de sus funciones requieran la habilitación de medios extraíbles de almacenamiento como son: almacenamiento USB, cámaras digitales, módems inalámbricos, unidades de almacenamiento CD/DVD y de dispositivos móviles; el responsable del órgano o unidad orgánica debe remitir el Anexo N° 01"Formato de Habilitación de Medios Extraíbles de Almacenamiento" firmado digitalmente por el Director/Jefe del órgano o la Unidad Orgánica correspondiente, justificando la necesidad. Adicionalmente el Anexo N° 02 "Acta de Confidencialidad para uso de Medios Extraíbles de Almacenamiento" firmado por el usuario final de la Directiva "Seguridad Informática de la red del RENIEC" a la Mesa de Ayuda de la OTI. Se exceptúa de esta disposición a los funcionarios de acuerdo con los lineamientos vigentes de "Seguridad Informática de la red del RENIEC".

b. Cuando se detecte una infección o ataque en progreso, originado por el uso del medio extraíble de almacenamiento, el usuario es responsable por los daños de software y/o hardware causados por la infección; en este caso se revoca el permiso correspondiente.

7.1.11. Servicios de suministro de apoyo (ISO 27001 A.7.11)

7.1.11.1. Para garantizar los servicios públicos sujetos a contingencias y que su ausencia o falla podrían afectar a los centros de datos como son: electricidad y telecomunicaciones; a fin de contribuir con la continuidad de los servicios de datos y que no sea interrumpida.

a. La OTI/UIST solicita ante la OAF, la operatividad del grupo electrógeno y coordina con la OSDN para que la Central de Monitoreo comunique a la OAF/USGCP cuando se presente una caída de fluido eléctrico.

b. La OTI/UIST realiza la formulación oportuna del requerimiento pertinente, para el uso de internet redundante considerando 2 proveedores alternos.

7.1.11.2. Los centros de datos en el RENIEC están protegidos contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.

7.1.11.3. La OAF/USGCP, coordina con las empresas de distribución eléctrica cuando se presenten mantenimientos preventivos y/o correctivos en la red de distribución por parte de la empresa de suministro de energía.

7.1.11.4. La OAF/USGCP, realiza periódicamente pruebas a los grupos electrógenos para su correcto funcionamiento.

7.1.12. Seguridad del cableado (ISO 27001 A.7.12)

7.1.12.1. La OTI/UIST, sigue los siguientes lineamientos:

a. Es responsable de realizar los diseños y supervisión de los sistemas de cableado estructurado en todas las sedes del RENIEC a nivel nacional. Así como las coordinaciones y acciones que sean necesarias para asegurar la continuidad y operatividad de este, en función a los recursos y capacidades disponibles.

b. Realiza el cableado estructurado de la red de acuerdo con un plano de distribución aprobado por la OAF/ USGCP y el órgano o unidad orgánica usuaria.

c. Garantiza la conectividad de la estación de trabajo siempre y cuando se mantenga en la ubicación definida de acuerdo con el plano de distribución.

7.1.12.2. Para la planificación y ejecución del mantenimiento preventivo de la Infraestructura de comunicaciones de los locales RENIEC a nivel nacional; asegurando la operatividad, continuidad y disponibilidad de los servicios del RENIEC en el lineamiento “Mantenimiento preventivo de la Infraestructura de Comunicaciones”.

7.1.12.3. Para realizar cambios de ubicación de los puntos de red, se debe coordinar con la OTI/UIST la verificación, evaluación y autorización correspondiente previa verificación de los planos de arquitectura que tuviese la OAF/USGCP y del aforo determinado por parte de la OSDN.

7.1.12.4. Asegurar los cables que transportan energía, datos o servicios de información de apoyo, estén protegidos contra intercepciones, interferencias o daños; para el caso de la energía eléctrica con la OAF/USGCP.

7.1.12.5. Asegurar el cableado en el RENIEC de la instalación subterránea con las protecciones debidas en las líneas de telecomunicaciones, evitando perturbaciones eléctricas dirigidas a las instalaciones de los centros de datos por parte de la OTI/UIST.

7.1.12.6. Asegurar las instalaciones eléctricas y de datos de acuerdo con las normas técnicas peruanas (NTP) eléctricas, y de

telecomunicaciones por parte de la OAF/USGCP y OTI/UIST.

7.1.12.7. Asegurar durante la identificación física y la inspección del cableado de datos, se etiquetan los cables en cada extremo con detalles de origen y destino.

7.1.13. Mantenimiento de equipos (ISO 27001 A.7.13)

7.1.13.1. La OTI/UIST realiza el "Mantenimiento preventivo y correctivo de equipos informáticos", garantizando así la operatividad y continuidad de los equipos informáticos del RENIEC.

7.1.13.2. Soporte Técnico de la OTI/UIST:

a. Mantiene los registros de todas las fallas y de todo mantenimiento preventivo y correctivo.

b. Gestiona un programa de mantenimiento de los equipos informáticos. Las reparaciones y mantenimiento de los equipos son realizados solo por personal de soporte autorizado.

7.1.13.3. Los equipos y servidores incluyen otros componentes como los UPS, extintores y aires acondicionados, los mismo que para su operatividad deben seguir un mantenimiento planificado ya sea con RENIEC o a través de un proveedor, siendo de responsabilidad de la OTI/UIST, OSDN y OAF/USGCP cuando corresponda.

7.1.14. Eliminación segura o reutilización de equipos (ISO 27001 A.7.14)

7.1.14.1. La OTI/UIST, establece en coordinación con la OAF/USGCP los lineamientos, a fin de que se evite fuga de información cuando se desechen, se reutilicen o se done equipos, ello debiéndose realizar en el marco de la normativa que resulte aplicable.

7.1.14.2. La OTI/UIST, define el lineamiento "Atención de requerimientos de soporte técnico", establece las acciones a seguir para la atención de requerimientos de soporte técnico de los equipos informáticos del RENIEC.

7.1.14.3. Para el caso de equipos dañados, estos pasan por una evaluación para determinar si se debe dar de baja o enviarse a reparar o desecharse, ello en coordinación previa con la OAF/USGCP.

7.1.14.4. Un equipo, antes de su reutilización o dado de baja o cuando culmine su arrendamiento, es verificado, si sus medios de almacenamiento están con contenido. En los casos de que un medio de almacenamiento contenga información confidencial o con derechos de autor, se procede a:

a. Destruir físicamente el medio de almacenamiento, ello en coordinación con la OAF/USGCP.

b. La información que contiene en los medios físicos de almacenamiento como discos duros, entre otros, debe

eliminarse o sobrescribirse utilizando técnicas para hacer que la información original no se pueda recuperar (formateo de bajo nivel).

VIII. DISPOSICIÓN COMPLEMENTARIA

8.1. Cualquier situación no contemplada en la presente Directiva, respecto a los controles físicos de seguridad de la información del RENIEC, debe ser informada por los Dueños de procesos, gestores de seguridad de la información, órganos y unidades orgánicas involucradas, a la OSCD para la gestión correspondiente.

8.2. En caso de incumplimiento por parte de los/las funcionarios/as o servidores/as de las obligaciones y prohibiciones dispuestas en la presente Directiva y otros documentos relacionados a los controles de seguridad de la información, facultan al RENIEC adoptar las medidas disciplinarias respecto del personal que los infringe, de acuerdo al régimen legal y de organización interna que las regula sin perjuicio de las responsabilidades civiles y penales que correspondan.

IX. VIGENCIA

La presente directiva entrara en vigor a partir de su aprobación.

X. APROBACIÓN

Mediante Resolución Secretarial.