DIRECTIVA

DI-037-SGEN/004

CONTROLES ORGANIZACIONALES DE SEGURIDAD DE LA INFORMACIÓN DEL SGSI - RENIEC

SEGUNDA VERSIÓN

SECRETARÍA GENERAL

ÍNDICE

I. OBJETIVO

Establecer los lineamientos que orienten a gestionar los controles organizacionales de la 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 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° 27815,** Ley del Código de Ética de la Función Pública, del 22 de julio de 2002 y sus modificatorias.

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

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

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

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

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

3.11. **Decreto Supremo N° 015-98-PCM**, Reglamento de las Inscripciones del Registro Nacional de Identificación y Estado Civil y sus modificatorias.

3.12. **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.

3.13. **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.

3.14. **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.

3.15. **Decreto Supremo N° 003-2013-JUS**, que aprueba el Reglamento de la Ley N°29733, Ley de Protección de Datos Personales, del 22 de marzo de 2013.

3.16. 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.

3.17. Decreto Supremo N° 092-2017-PCM, que aprueba la Política Nacional de Integridad y Lucha Contra la Corrupción, del 14 de setiembre de 2017.

3.18. 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.

3.19. Decreto Supremo N° 042-2018-PCM, que establece medidas para Fortalecer la Integridad Pública y Lucha Contra la Corrupción del 22 de abril de 2018.

3.20. Decreto Supremo N° 044-2018-PCM, que aprueba el Plan Nacional de Integridad y Lucha Contra la Corrupción 2018-2021, del 26 de abril de 2018; mantiene su vigencia según lo dispuesto en el Decreto Supremo N° 180-2021-PCM del 10 de diciembre de 2021.

3.21. 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.

3.22. 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.

3.23. 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.

3.24. 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, y su modificatoria.

3.25. 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.

3.26. 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.

3.27. 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.

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

3.29. 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.

3.30. 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.

3.31. 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.

3.32. 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.

3.33. 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.

3.34. 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.

3.35. 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.

3.36. Resolución Jefatural Nº 000061-2024/JNAC/RENIEC, que aprueba el Reglamento de Organización y Funciones y la Estructura Orgánica del Registro Nacional de Identificación y Estado Civil - RENIEC, del 8 de abril de 2024.

3.37. Resolución Secretarial Nº 000084-2024/SGEN/RENIEC, que aprueba la Directiva DI-001-OPPM/001 “Documentos normativos del RENIEC”, primera versión, del 8 de julio de 2024.

3.38. Norma Internacional ISO/IEC 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 de octubre de 2022.

3.39. Norma Internacional ISO/IEC 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

En la presente Directiva se utilizan las siguientes abreviaciones y siglas:

ABREVIATURA	NOMBRE
RENIEC	Registro Nacional de Identificación y Estado Civil
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
ROF	Reglamento de Organización y Funciones
CISO	Chief Information Security Officer (Director/a de seguridad de la información)
OPDP	Oficial de Protección de Datos Personales
RUIPIN	Registro Único de Identificación de las Personas Naturales
SGTD	Secretaría de Gobierno y Transformación Digital
TIC	Tecnologías de la Información y Comunicaciones

SIGLAS DE LAS UNIDADES DE ORGANIZACIÓN DEL RENIEC	
JNAC	Jefatura Nacional
GG	Gerencia General
SGEN	Secretaría General
OSDN	Oficina de Seguridad y Defensa Nacional
OILCC	Oficina de Integridad y Lucha contra la Corrupción
OPPM	Oficina de Planeamiento, Presupuesto y Modernización
OAJ	Oficina de Asesoría Jurídica
OAF	Oficina de Administración y Finanzas
OPH	Oficina de Potencial Humano
OTI	Oficina de Tecnologías de la Información
OGD	Oficina de Gestión Documental
UGTI	Unidad de Gobierno de Tecnologías de la Información
UIST	Unidad de Infraestructura y Soporte Tecnológico
UIS	Unidad de Ingeniería de Software
ULG	Unidad de Logística
USGCP	Unidad de Servicios Generales y Control Patrimonial
USTPAD	Unidad de Secretaría Técnica de Procedimientos Administrativos Disciplinarios
DCSD	Dirección de Certificación y Servicios Digitales
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.	

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. Alta Dirección
Está conformado por la Jefatura Nacional, Gerencia General y Secretaría General.

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

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

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

4.7. Etiquetado
Es el acto de rotular o marcar el medio de soporte y/o unidad de archivamiento de acuerdo al nivel de clasificación de la información que contiene.

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

4.9. Incidente de Seguridad de la Información[1]
Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de una organización o comprometer sus operaciones y amenazar la seguridad de la información de la entidad pública.

4.10. Incidente de Seguridad Digital[2]
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.

4.11. Propietario del activo
El propietario de un activo de información puede ser un individuo o una entidad que a la que la dirección ha asignado la responsabilidad de gestionar el activo en su ciclo de vida completo.

4.12. Disrupción
Incidente ya sea anticipado o no, que causa una desviación negativa no planificada de la entrega esperada de productos y servicios de acuerdo a los objetivos de una organización.

4.13. Integridad
Propiedad de exactitud e integridad.

4.14. 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,

[1] Norma Técnica Peruana NTP-ISO/IEC 27002:2022
[2] Decreto de Urgencia N°007 – 2020

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 del servidor civil.

4.15. Plan de Recuperación de Desastres

El Plan de Recuperación de Desastres DRP (Disaster Recovery Plan) corresponde a las áreas de tecnologías de información. Es diseñado para gestionar como la organización puede recuperar el trabajo de manera rápida, después de un incidente no programado, con el objetivo de resolver la perdida de datos y recuperar la funcionalidad del sistema. Este plan es una parte esencial del Plan de Continuidad Operativa del RENIEC.

4.16. Riesgo

Efecto de la incertidumbre sobre los objetivos.

4.17. Servidor/a civil

Toda persona que tiene un vínculo laboral o contrato administrativo de servicio con el Estado. Es el usuario interno del RENIEC.

4.18. Servidor informático

Equipo informático que almacena, distribuye y suministra información.

4.19. Sistema de Gestión de Seguridad de la Información SGSI

Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para lograr los objetivos comerciales. Se basa en una evaluación de riesgos y los niveles de aceptación de riesgos de la organización diseñados para tratar y gestionar los riesgos de forma eficaz. Analizar los requisitos para la protección de los activos de información y aplicar controles adecuados para garantizar la protección de estos activos de información, según sea necesario, contribuye a la implementación exitosa de un SGSI; y consta de políticas, procedimientos, directrices, recursos y actividades asociados, gestionados colectivamente por una organización, en la búsqueda de proteger sus activos de información.

4.20. Software

Conjunto de programas o aplicación informáticos desarrollados o adquiridos por el RENIEC.

V. RESPONSABILIDADES

En función de los controles organizacionales de seguridad de la información del SGSI, se establecen las responsabilidades de los Dueños del Proceso, órganos y unidades orgánicas involucradas[3], de acuerdo a las funciones conferidas en el ROF del RENIEC y normativa vigentes.

5.1. Jefatura Nacional JNAC

Es responsable de aprobar la política y objetivos de seguridad de la información del SGSI - RENIEC, mediante Resolución Jefatural.

[3] Los controles de seguridad de la información, son identificados en la Tabla A.1 Controles de Seguridad de la Información, numeral 5. Controles Organizacionales, 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.

5.2. Gerencia General GG

Asegurar y monitorear la implementación, mantenimiento, desempeño y funcionamiento de los Sistemas de Gestión, así como el cumplimiento de sus procesos, procedimientos y actividades de los órganos y unidades orgánicas de línea.

5.3. Secretaría General SGEN

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.

5.4. Oficina de Seguridad y Defensa Nacional OSDN

Es responsable, de supervisar el cumplimiento de los controles relacionados con la gestión del sistema de seguridad institucional, que garantice la protección de las personas, los bienes, las instalaciones y el normal funcionamiento de los servicios de la institución; los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.

5.5. Oficina de Integridad y Lucha contra la Corrupción OILCC

Es responsable de coordinar con los diferentes órganos y unidades orgánicas de la institución la aplicación del marco normativo para la gestión del riesgo: identificación, análisis, valoración, tratamiento y seguimiento de los riesgos, revisar y actualizar el marco normativo para gestión del riesgo en la institución.

5.6. Oficina de Planificación, Presupuesto y Modernización OPPM

Es responsable, a través de sus unidades adscritas (Unidad de Planeamiento e Inversiones, Unidad de Presupuesto y Unidad de Modernización Organizacional), orientar a la OSCD para asegurar una adecuada articulación de los instrumentos de gestión institucional, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.

5.7. Oficina de Asesoría Jurídica OAJ

Es responsable de cumplir con los controles de seguridad de la información, relacionados a la asistencia técnica de carácter jurídico, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.

5.8. Oficina de Administración y Finanzas OAF

Es responsable de normar, según el marco legal vigente dentro del Sistema Nacional de Abastecimiento, el proceso de salida de la entidad de los bienes muebles patrimoniales de naturaleza informática, los cuales se realizan por motivos de teletrabajo, desplazamientos externos por diversas causas, entre otros relacionados y afines solo para uso institucional; así como normar las responsabilidades de los usuarios, dando lineamientos sobre el debido uso de los equipos informáticos de la entidad, a efecto de que se lleve un adecuado control a través de la Unidad de Servicios Generales y Control Patrimonial, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.

5.9. Oficina de Potencial Humano OPH

Es responsable de gestionar el recurso humano de la institución, en relación a la capacitación, seguridad y salud en el trabajo; así como gestionar los procesos administrativos disciplinarios, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.

5.10. Oficina de Comunicaciones y Prensa

Es responsable de supervisar y evaluar las políticas y estrategias de la gestión de comunicación institucional, comunicación digital, prensa, publicidad, protocolo, relaciones institucionales y acciones de responsabilidad social; velando por la identidad, la imagen y la reputación de la institución[4], los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.

5.11. Oficina de Tecnologías de la Información OTI

Es responsable, a través de sus unidades adscritas (Unidad de Infraestructura y Soporte Tecnológico, Unidad de Gobierno de Tecnologías de la Información, y Unidad de Ingeniería de Software) del soporte tecnológico de la institución a nivel nacional e internacional, encargada de brindar servicios de tecnología de la información y comunicación oportuna y veraz, promoviendo el uso ético de las tecnologías digitales; así como de informar al Oficial de Seguridad y Confianza Digital (OSCD) todo incidente de seguridad digital crítico que afecte los procesos misionales y servicios que brinda la entidad, de forma inmediata. Asimismo, articula con el OSCD la implementación de controles de seguridad de la información y coordina con el Equipo de Respuestas ante Incidentes de Seguridad Digital la gestión de incidentes de seguridad digital.

5.12. Unidad de Infraestructura y Soporte Tecnológico UIST

Es responsable de cumplir con los controles de seguridad de la información, con relación a los servicios informáticos internos y externos, funcionamiento de la base de datos y redes de comunicaciones, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.

5.13. Unidad de Gobierno de Tecnologías de la Información UGTI

Es responsable, de coordinar las acciones de implementación y mantenimiento de controles de seguridad digital en el marco del Sistema de Gestión de Seguridad de la Información - SGSI; los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.

5.14. Unidad de Ingeniería de Software UIS

Es responsable de cumplir con los controles de seguridad de la información, relacionados a la planificación y desarrollo de los sistemas informáticos, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.

5.15. Oficina de Gestión Documental OGD

Es responsable de cumplir con los controles de seguridad de la información, relacionados con la administración del modelo de gestión documental de la institución, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.

5.16. Dirección de Certificación y Servicios Digitales DCSD

Es responsable de cumplir con los controles de seguridad de la información, relacionados a la seguridad para el acceso a la información de Consultas

[4] Control 5.5 Contacto con autoridades_ La organización debe establecer y mantener contacto con las autoridades pertinentes.

RENIEC, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.

5.17. Oficial de Protección de Datos Personales OPDP

El ODP interviene como enlace con la Autoridad Nacional de Protección de Datos Personales (ANPD), coopera y efectúa seguimiento a los lineamientos y directivas que emita dicha Autoridad, así como aquellos establecidos en el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital; y dispone medidas para su fortalecimiento.

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

5.18.1. Coordinar la implementación, operación, mantenimiento y mejora continua del SGSI del RENIEC[5].

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

5.18.3. Formular y actualizar la presente Directiva y procedimientos en materia de Seguridad de la Información acorde a la normativa vigente.

5.18.4. Informar a través de 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 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, proponer o actualizar los controles organizacionales de seguridad de la información contenidos en la presente Directiva, en coordinación con el OSCD, OPDP y con los OO. y UU. OO involucradas según corresponda[6].

6.2. La OSDN gestiona el sistema de control de visitas - PCM y supervisa el servicio que brindan las empresas de seguridad y vigilancia en las instalaciones de la institución.

6.3. La OPPM gestiona el control relacionado a los planes, programas y documentos de gestión interna de la institución.

6.4. La OAJ gestiona el control relacionado a requisitos legales, estatutarios, regulatorios y contractuales.

6.5. La OAF gestiona los controles relacionados a derechos de acceso, seguridad de la información en las relaciones con los proveedores y abordar la seguridad de la información en los acuerdos con los proveedores.

6.6. La OPH gestiona el recurso humano de la institución, así como lo relacionado al Sistema de Gestión de la Seguridad y Salud en el Trabajo - SGSST,

[5] Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD _ Directiva N° 001-2023-PCM/SGTD, Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital.

[6] SGEN, GG, OPPM, OAJ, OAF, OPH, OSDN, OGD, OILCC, OTI, DCSD y otros involucrados.

asegurando las condiciones de trabajo que garanticen la salud y seguridad ocupacional en coordinación con el Comité designado por la Alta Dirección.

6.7. La OTI/UIST gestiona los controles relacionados a inteligencia de amenazas, transferencia de información, control de acceso, gestión de identidades, información de autenticación, derechos de acceso, seguridad de la información en las relaciones con los proveedores, gestión de la seguridad de la información en la cadena de suministro de las tecnologías de la información y la comunicación (TIC), seguridad de la información en el uso de servicios en la nube, preparación de las TIC para la continuidad del negocio, derechos de propiedad intelectual, protección de los registros, procedimientos operativos documentados.

6.8. La OTI/UGTI gestiona los controles relacionados a las acciones de implementación y mantenimiento de seguridad digital en el marco del Sistema de Gestión de Seguridad de la Información - SGSI[7].

6.9. La OTI/UIS gestiona los controles relacionados a inteligencia de amenazas, información de autenticación y derechos de propiedad intelectual.

6.10. La OGD gestiona los controles relacionados a clasificación de la información, transferencia de información y protección de los registros.

6.11. La DCSD gestiona el control relacionado a seguridad para el acceso a la información de Consultas - RENIEC.

6.12. El OPDP gestiona el control relacionado a privacidad y protección de la información de identificación personal.

6.13. La OSCD gestiona los controles relacionados a políticas para la seguridad de la Información, roles y responsabilidades en seguridad de la información, contacto con grupos especiales de interés, inteligencia de amenazas, clasificación de la información; así como aborda la seguridad de la información en los acuerdos con los proveedores, evalúa en coordinación con los órganos y unidades responsables sobre los eventos de seguridad de la información, requisitos legales, estatutarios, regulatorios y contractuales, Derechos de propiedad intelectual, revisión independiente de la seguridad de la información y cumplimiento con políticas, reglas y normas de seguridad de la información y seguridad para el acceso a la información de Consultas RENIEC.

Asimismo, coordina con la OILCC los lineamientos relacionados en materia de gestión de riesgos de seguridad de la información; tales como activos de información, clasificación de la información, entre otros que sean pertinentes, para la actualización de los documentos normativos que correspondan.

VII. DISPOSICIONES ESPECÍFICAS

Los controles organizacionales de la seguridad de la información son transversales a los procesos de la institución y han sido desarrollados en cumplimiento de los requisitos del Anexo A Tabla A.1 Controles de seguridad de la información de la 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 organizacionales (ISO 27001 A.5)

7.1.1. Políticas para la Seguridad de la Información (ISO 27001 A.5.1)

7.1.1.1. La SGEN a través del OSCD propone la política de seguridad de la información y es revisada por el Comité de

[7] Revisión independiente de la seguridad de la información revisión independiente de la seguridad de la información.

Gobierno y Transformación Digital quien a su vez eleva a la instancia correspondiente, para la aprobación de la JNAC mediante Resolución Jefatural.

7.1.1.2. La política de seguridad de la información establece el enfoque de la organización para gestionar los objetivos de seguridad de la información, publicada y difundida, para conocimiento y aplicación de los servidores civiles de la organización y acceso de las partes externas relevantes. Asimismo, la política de seguridad de la información es revisada de forma periódica (cada año) o cuando ocurran cambios significativos de la NTP o normativa legal.

7.1.2. Roles y responsabilidades en Seguridad de la Información (ISO 27001 A.5.2)

7.1.2.1. Los roles y responsabilidades en la organización, en cuanto a seguridad de la información, son propuestas por la SGEN a través del OSCD[8], y aprobadas por la Alta Dirección, bajo una estructura organizativa detallada en el "Manual de Gestión de Seguridad de la Información".

7.1.3. Segregación de funciones (ISO 27001 A.5.3)

7.1.3.1. El RENIEC, cuenta con:

a. El Reglamento de Organización y Funciones y Estructura Orgánica - ROF, donde se detallan las funciones, responsabilidades y niveles de la estructura de la entidad.

b. El Manual de Clasificador de Cargos del Registro Nacional de Identificación y Estado Civil - RENIEC MCC, en el que se describen de manera ordenada todos los cargos de la entidad, estableciendo su denominación, clasificación, funciones y requisitos mínimos para el cumplimiento de objetivos de la entidad.

7.1.3.2. La segregación de funciones es un método de control basado en roles; con el fin de definir la actividad a desarrollar por cada integrante de la estructura organizativa de la institución; para el caso del SGSI los roles y responsabilidades se encuentran detallados en el "Manual de Gestión de Seguridad de la Información", documento que señala que los dueños de los procesos disponen de una matriz de requisitos de competencias[9], el mismo que define el perfil de formación académica y tecnológica de preferencia para el personal relacionado con las labores de seguridad de la información.

[8] 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.

[9] Anexo "Matriz de Requisitos de competencia para Roles" del Manual de Gestión de Seguridad de la Información" para personal propuesto para labores de seguridad de la información.

7.1.4. Responsabilidades de la Dirección (ISO 27001 A.5.4)

7.1.4.1. La Alta Dirección manifiesta su compromiso con la Seguridad de la Información, dando cumplimiento con las siguientes acciones:

a. Aprobar la política de Seguridad de la Información.

b. Impulsar la aplicación de la seguridad de la información a todos los Dueños del proceso, órganos y unidades orgánicas sobre la base de la Política y Objetivos de Seguridad de la Información del RENIEC.

7.1.5. Contacto con autoridades (ISO 27001 A.5.5)

7.1.5.1. La OCP supervisa y evalúa las políticas y estrategias de la gestión de comunicación institucional, comunicación digital, prensa, publicidad, protocolo, relaciones institucionales y acciones de responsabilidad social; velando por la identidad, la imagen y la reputación de la institución.

Asimismo, evalúa la relación de la institución con los medios de comunicación, entidades públicas o privadas de carácter regional, nacional e internacional; así como otras asociaciones y organizaciones no gubernamentales.

7.1.5.2. La OPH gestiona acuerdos o convenios de cooperación interinstitucional con entidades públicas o privadas, nacionales o extranjeras, en el ámbito de su competencia en beneficio de los servidores en coordinación con el órgano o unidad orgánica competente para dicho fin.

7.1.5.3. La DCSD gestiona los convenios de suministro de información con entidades privadas y públicas a ser suscritos, y los servicios disponibles de la institución.

7.1.6. Contacto con grupos especiales de interés (ISO 27001 A.5.6)

7.1.6.1. En el contexto del SGSI, se establece y mantiene contacto con grupos de interés especial y otras asociaciones profesionales especializadas en seguridad con la finalidad de garantizar el intercambio de información referente a la seguridad de la información, tales como foros, páginas web informativas, enlaces a videos, grupos de mensajería, entre otros.

7.1.6.2. La SGEN a través del OSCD[10], procede a:

a. Definir y actualizar los grupos de interés especial pertinentes para el SGSI, una vez al año o cuando ocurran cambios, y la respectiva lista se difunde a los procesos correspondientes, de acuerdo con el formato establecido en el Anexo N° 02 “Contacto con grupos de interés especial del Sistema de Gestión de Seguridad de la Información” de la presente directiva.

b. Recibir comunicación respecto a seguridad de información, así mismo mantiene constante relación con las entidades externas que puedan prestar apoyo

[10] El OSCD se encuentra registrado en el grupo de CISO de las entidades públicas a través del recibe información calificada.

en caso de incidentes de seguridad de la información, pero sin generar obligaciones de entregar información confidencial.

7.1.7. Inteligencia de amenazas (ISO 27001 A.5.7)

7.1.7.1. La SGTD[11] emite alertas al OSCD, responsables técnicos de seguridad informática o de ciberseguridad sobre las amenazas de seguridad digital que vienen afectando a las entidades públicas y empresas.

7.1.7.2. El OSCD envía las alertas de seguridad digital al Gestor Líder de la OTI.

7.1.7.3. La OTI a través de la UIST y UIS, recibe y atiende lo reportado por el OSCD, tanto las alertas de seguridad digital, como los comunicados de la SGTD; la misma que tienen por objeto informar a los responsables técnicos de seguridad informática.

7.1.7.4. El servicio de ciberseguridad es gestionado por la OTI/UIST, unidad que realiza el seguimiento permanente y emite una alerta diaria de la información publicada y circulante en internet (Webs convencionales, redes sociales, páginas de hacking y blogs); así como en la Deep Web que puedan ocasionar incidentes de seguridad de la información, la misma que gestiona para dar respuesta inmediata a estas amenazas[12].

7.1.8. Seguridad de la información en la Gestión de Proyectos (ISO 27001 A.5.8)

7.1.8.1. El Gestor del Proyecto debe:

a. Gestionar el proyecto y los recursos asociados a éste con la finalidad de cumplir los objetivos del mismo.

b. Formalizar la asignación y/o conformación de un equipo, y este debe estar integrado por un miembro de la OTI y el OSCD en caso amerite por el uso de datos sensibles.

c. Incorporar a los funcionarios, gestores líderes, operativos, especialistas de seguridad de información y/u otra designación de los procesos que son impactados para el proyecto, los mismos que tendrán como función dentro del proyecto la identificación de riesgos que impacten a los activos de seguridad de información, así como el continuo seguimiento de estos, de acuerdo con lo establecido en el documento normativo “Gestión Integral de Riesgo”.

[11] La Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros (PCM) lidera la articulación, implementación y evaluación de la Política Nacional de Transformación Digital y su estrategia, así como las políticas nacionales, planes nacionales, normas, lineamientos, proyectos y plataformas para tal fin.
[12] La OTI/UIST realiza el seguimiento de las alertas reportadas.

7.1.9. Inventario de información y otros activos asociados (ISO 27001 A.5.9)

7.1.9.1. El inventario de activos de información es desarrollado por cada proceso utilizando el formato “Inventario de activos de información”, conforme a los lineamientos y normativa vigentes, para la gestión de riesgos de seguridad de la información.

7.1.9.2. Los Dueños del proceso, órganos y unidades orgánicas del RENIEC, deben determinar las responsabilidades a realizar para la actualización del inventario de activos de información, anualmente o cuando ocurra algún cambio en los procesos o activos.

7.1.10. Uso aceptable de la información y otros activos asociados (ISO 27001 A.5.10)

7.1.10.1. Todos los activos de información deben ser utilizados considerando lo siguiente:

a. El propósito expreso de realizar tareas relacionadas a las actividades del RENIEC.

b. Uso adecuado, cualquiera sea el medio que los soporte y el ambiente en que se procesen.

c. Ante la presencia de terceros en lugares públicos (ambientes de la entidad accesible a terceros), el servidor civil no debe tratar información de manera presencial o telefónicamente, respecto a temas sensibles que correspondan a información confidencial.

d. Los propietarios del activo de la información registral deben controlar que dicha información sea accedida únicamente por el personal de la entidad debidamente autorizados y que cuente con los privilegios adecuados.

7.1.11. Devolución de activos (ISO 27001 A.5.11)

7.1.11.1. Mediante documento normativo “Entrega de puesto de los servidores civiles del RENIEC”, se establecen las pautas para la entrega de puesto, el cual contempla entre otros la entrega de activos de información de acuerdo con el Anexo N° 1, Acta de Entrega de Puesto.

7.1.11.2. Los Dueños del Proceso, Órganos y Unidades Orgánicas del RENIEC al cual pertenece, un servidor civil sujeto a traslado o extinción del contrato, evita que se realicen copias no autorizadas de la información de la organización y/o del proceso, a través del retiro inmediato de los permisos asignados en los sistemas o carpetas compartidas en el servidor informático de la OTI/UIST.

7.1.11.3. El servidor civil y otras partes interesadas, según corresponda, realizan la devolución de los activos de la organización (ya sea de información, equipos y de acceso a sistemas) que estén en su poder, en casos de cambio de empleo o culminación de contrato; evitando tener copias no autorizadas en su custodia personal.

7.1.12. Clasificación de la información (ISO 27001 A.5.12)

7.1.12.1. La OGD, establece el procedimiento a seguir para la atención de solicitudes de acceso a la información pública, teniendo en cuenta las disposiciones de la Ley N° 27806 “Ley de Transparencia y Acceso a la Información Pública” y su reglamento.

7.1.12.2. La clasificación de los activos de información es desarrollada por cada proceso utilizando el formato “Inventario de activos de información".

7.1.12.3. La clasificación, tratamiento y desclasificación de la información en los órganos y unidades orgánicas del RENIEC se establece en concordancia con el Sistema de Gestión de Seguridad de la Información, normas de transparencia y acceso a la información pública.

Responsabilidad de la clasificación:

a. Cada Unidad Orgánica clasifica y desclasifica la información secreta, reservada y confidencial del RENIEC, que se refiere el Texto Único Ordenado por Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, su Reglamento y modificatoria, aprobados por los Decretos Supremos N° 43-2013-PCM, 72-2003-PCM y 70-2013-PCM.

b. La OGD ejecuta las acciones orientadas al cumplimiento de los procesos técnicos archivísticos (organización, conservación, transferencia y eliminación) y a la custodia del patrimonio documental del RENIEC, en concordancia con los documentos normativos del Archivo General de la Nación.

c. La OGD propone las medidas de seguridad de la documentación que se custodia en el sistema de archivo institucional, que permita la protección, conservación e incremento del patrimonio documental de la institución en coordinación con la OTI.

7.1.12.4. Es responsabilidad del Gestor Líder de seguridad de la información de cada proceso, coordinar con los funcionarios las acciones para la clasificación de la información, etiquetado y uso adecuado de los activos de seguridad de la información con la OSCD.

7.1.12.5. Es responsabilidad del Gestor Operativo de Seguridad de la Información:

a. Elaborar la clasificación de activos de información del Órgano o Unidad Orgánica asignada.

b. Gestionar la implementación de controles de seguridad de la información según la clasificación establecida.

7.1.12.6. El proceso para dejar sin efecto la clasificación de los activos de información se realiza a solicitud del Propietario de la Información en coordinación con el responsable del órgano o unidad orgánica, o viceversa.

7.1.13. Etiquetado de la información (ISO 27001 A.5.13)

7.1.13.1. Los gestores de seguridad de la información designados por el Órgano o Unidad Orgánica deben asegurarse que los activos de información definidos como “Confidencial”, “Reservada” y “Secreta” lleven un rótulo que identifique su nivel de clasificación.

7.1.13.2. La rotulación de los activos de información se realiza de forma estandarizada para los activos que se encuentran en los sistemas de información y estos a su vez en servidores informáticos; se colocará una etiqueta en los activos físicos que los contenga. Para el caso de activos electrónicos que no se encuentren almacenados en los servidores informáticos se les colocará un pie de página “confidencial” como, por ejemplo: “Plan de Gestión Integral del Riesgo del Sistema de Gestión de Seguridad de la Información”.

7.1.14. Transferencia de información (ISO 27001 A.5.14)

7.1.14.1. La transferencia de información puede ocurrir a través de transferencia electrónica, y transferencia de medios de almacenamiento físico.

7.1.14.2. La OGD tiene a su cargo el modelo de Gestión Documental dispuesto por norma:

- Recepción (Mesa de Partes)
- Derivación (SITD)
- Entrega (Notificación)
- Archivo

7.1.14.3. La OGD gestiona sus cuatro procesos de acuerdo a normas dispuestas por la SGTD Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, el Archivo General de la Nación y directivas internas.

7.1.14.4. La transmisión de datos, archivos y documentos electrónicos está garantizada por las medidas de seguridad propias de la gestión de la seguridad de la red que se indica en la presente directiva, la transmisión se realiza a través de la red privada y pública de acuerdo a los siguientes aspectos:

a. En la red privada se transmiten datos, archivos y documentos electrónicos a los servidores de aplicaciones, servidores de bases de datos, servidores de almacenamiento y las estaciones de trabajo de la línea de producción de Microformas Digitales y las estaciones remotas del RENIEC.

b. En la red pública se transmiten los servicios de consultas de datos que brinda RENIEC únicamente a instituciones que cuenten con direccionamiento IP público con origen en Perú, a excepción de los Consulados del Perú.

7.1.14.5. Se debe obtener aprobación del responsable del órgano o unidad orgánica, antes de utilizar servicios públicos externos en la red corporativa, como mensajería instantánea, redes sociales, uso compartido de archivos o almacenamiento en la nube; por lo tanto, la OTI/UIST bloqueara estos servicios por defecto.

7.1.14.6. La transmisión libre de interceptaciones entre las estaciones emisoras y receptoras está garantizada por el uso de Certificados Digitales, control de accesos, políticas de Grupo y perfiles de usuario, entre otros mecanismos contemplados en la presente Directiva.

7.1.14.7. Para las operaciones de transferencias de los registros electrónicos, archivos y datos, el sistema genera automáticamente información (log files, log del sistema, log de servidores informáticos), donde se encuentran registrados la fecha y hora de transferencia.

7.1.15. Control de acceso (ISO 27001 A.5.15)

7.1.15.1. La OSDN define los documentos normativos para el control de acceso físico, en la directiva DI-206-OSDN/001 “Seguridad de las instalaciones en sedes, oficinas registrales, agencias, locales y/o puntos de atención”, donde se establecen las acciones a seguir en aspectos relativos a la seguridad en las instalaciones, con el mobiliario, material documentario y equipos; así como, el ingreso y tránsito del servidor civil, visitas y/o contratistas a las sedes, oficinas registrales, agencias, locales y/o puntos de atención. Para el control de acceso físico está también los documentos normativos, GP-344-OSDN/004 “Ingreso de contratistas, visitantes y personal del RENIEC en días y horarios no laborables, a las instalaciones del RENIEC", que establece las acciones a seguir para solicitar, verificar y controlar el ingreso de los contratistas y visitantes a las instalaciones del RENIEC, así como, del servidor civil del RENIEC en horarios regulares y días no laborables. Por último, mediante la NAI-386-OSDN “Normas y Obligaciones del Personal de Vigilancia”, se establecen pautas para el personal de las empresas de vigilancia.

7.1.15.2. La OTI/UIST, es responsable de la creación, administración y desactivación de los usuarios para acceso a la red, por lo cual el acceso a los recursos informáticos internos y los sistemas de información del RENIEC es a través de usuarios y contraseñas. Estas tareas deben estar acordes a la norma de administración de cuentas y claves de acceso. La deshabilitación del usuario se debe realizar en 24 horas como máximo, luego de la comunicación de OPH.

7.1.15.3. La autorización de acceso a la información, por parte de los usuarios se debe realizar de acuerdo con sus atribuciones, funciones y/o tareas a desarrollar. Estas son asignadas por el responsable del órgano o unidad orgánica que corresponda; quién será el responsable de definir el perfil de acceso del servidor civil a su cargo.

7.1.15.4. En caso el Gobierno, decrete documentos normativos debido al estado de emergencia, emergencias sanitarias, entre otros y se requiera coordinar con otras entidades el servicio de suministro de información, implica, que, se debe contar con la autorización de la Alta Dirección del RENIEC a fin de proceder con las coordinaciones para el cumplimiento de las disposiciones emitidas y generar la evidencia correspondiente al desarrollo de actividades a realizar.

7.1.15.5. Los equipos para servicios de Telefonía, Videoconferencia y Videovigilancia IP deben estar protegidos con dispositivos bloqueadores de puerto físicos, para garantizar la seguridad de la infraestructura.

7.1.16. Gestión de identidades (ISO 27001 A.5.16)

7.1.16.1. El responsable del órgano o unidad orgánica designa a los usuarios que accederán a las aplicaciones del RENIEC.

7.1.16.2. La OTI/UIST, está a cargo de la administración del registro y baja de la identidad de los usuarios, bajo las consideraciones siguientes:

a. Una identidad específica se vincula a una sola persona para poder responsabilizarla por las acciones realizadas con esa identidad específica.

b. Las identidades asignadas a usuarios se deshabilitan o eliminan de manera oportuna si ya no son necesarias (si el usuario ha dejado la organización o ha cambiado de función o a solicitud del órgano o unidad orgánica).

c. Se debe mantener registro de todos los eventos y de su trazabilidad, relacionados con el uso y la gestión de las identidades de los usuarios y de la información de autenticación.

7.1.16.3. La OTI, define las disposiciones de la gestión de los usuarios del RENIEC, en el documento normativo "Servicios de comunicación para usuarios finales", que establece la pautas a seguir para el uso de los servicios de perfil de dominio, correo institucional, mensajería interna, acceso a internet, y el documento normativo "Solicitud de creación, activación, desactivación y cambio de nivel de usuarios", que establece las pautas para el acceso a los niveles de usuarios en las aplicaciones informáticas del RENIEC.

7.1.16.4. Las contraseñas representan un factor fundamental de la seguridad de los recursos informáticos, siendo la primera línea de protección básica para el usuario y para la red.

7.1.16.5. La cuenta de usuario y su contraseña es de carácter personal e intransferible, está prohibido compartir a terceras personas. Por lo tanto, se prohíbe solicitar el reseteo de la contraseña de una cuenta de dominio distinto a su titular.

7.1.16.6. Para la autenticación con el DNIe, se requiere previamente asociar el certificado digital contenido en el chip del DNIe con el perfil de dominio del usuario.

7.1.17. Información de autenticación (ISO 27001 A.5.17)

7.1.17.1. La OTI/UIST, establece los siguientes lineamientos:

a. Las contraseñas personales o los números de identificación personal (PIN) generados automática y aleatoriamente, son únicos para cada persona y los usuarios deben cambiarlos después del primer uso.

b. La información de autenticación secreta, como las contraseñas, se mantiene confidencial, por lo tanto, no debe compartirse.

c. La información de autenticación se trasmite a los usuarios de manera segura, evitando el uso de mensajes de correo institucional sin protección para este propósito; acusando recibo por parte del usuario, de ser necesario.

d. Toda contraseña afectada o comprometida se debe cambiar inmediatamente después de la notificación o sospecha.

e. Las contraseñas deben tener letras mayúsculas y minúsculas, números y/o caracteres especiales; además de tener una longitud mínima de ocho caracteres.

f. El sistema de administración de contraseñas es interactivo y asegura que las contraseñas cumplan con lo siguiente:

- Permitir que el usuario cambie sus propias contraseñas, incluyendo un procedimiento de confirmación para abordar los errores de estos.
- Obligar al usuario a cambiar su contraseña en el primer inicio de sesión.
- Evitar la reutilización de contraseñas anteriores como mínimo 10 veces.
- No mostrar contraseñas en la pantalla cuando se ingresan.
- Almacenar y trasmitir contraseñas en forma protegida, a través de un canal seguro.

7.1.17.2. La OTI/UIS, implementa el MFA (autenticador multifactor) de acuerdo con su criticidad o sensibilidad de la información, utilizando alguno de los 3 tipos básicos de factores de autenticación que existen: Algo que sabes (contraseña, pin, etc.) y/o algo que tienes (token usb, smartcard, app, etc.) y/o algo que eres (biometría). Asimismo, la OTI/UIS, debe implementar la autenticación única utilizando el Active Directory (AD) para las aplicaciones alternas.

7.1.18. Derechos de acceso (ISO 27001 A.5.18)

7.1.18.1. Los dispositivos o recursos de telecomunicaciones en el tratamiento de la información tienen configuradas rutas establecidas (predefinidas) y dominios lógicos de acceso al sistema, los cuales están segmentados y divididos, tomando como premisa el control de acceso a la red y los objetivos principales de la Institución.

7.1.18.2. Se aplican medidas de control a los dispositivos de la red para su protección y acceso, para evitar que usuarios no autorizados puedan modificar las configuraciones establecidas.

7.1.18.3. El responsable del órgano o unidad orgánica define los derechos de acceso a la información y otros activos asociados, se proporciona, revisa, modifica y elimina de acuerdo con las políticas y las reglas de control de acceso que existen en el RENIEC, además de ser validados con la real necesidad de funciones y accesos por el responsable del órgano o unidad orgánica.

7.1.18.4. La OTI/UIST, establece los documentos normativos para el uso de los servicios de perfil de dominio, correo institucional, mensajería interna, acceso a internet, acceso a los sistemas de información (interno y externo), entre otros, en el documento normativo "Servicios de comunicación para usuarios finales", y en la "Solicitud de creación, activación, desactivación y cambio de nivel de usuarios", los mismos que establecen disposiciones para el acceso a los niveles de usuarios en las aplicaciones informáticas del RENIEC.

7.1.18.5. La OAF/ULG, para el caso de los proveedores de servicio, notifica a la OTI/UIST las culminaciones de los servicios y/o los desistimientos de servicios presentados, a fin de que se inicie el procedimiento de deshabilitación de usuarios.

7.1.19. Seguridad de la información en las relaciones con los proveedores (ISO 27001 A.5.19)

7.1.19.1. La OAF/ULG, realiza el proceso de adquisición de bienes y servicios en cumplimiento de la Ley de Contrataciones del Estado y su Reglamento. Asimismo, debe dar a conocer la Política de Seguridad de la Información del RENIEC a los proveedores.

7.1.19.2. El ingreso de equipos de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que sean de propiedad del proveedor deben ser registrados de acuerdo con la GP-325-OSDN/003 "Control de visitas en las sedes administrativas, operativa, Registros Civiles y Jr. Ancash" y la GP-344-OSDN/004 "Ingreso de contratistas, visitantes y personal en días y horarios no laborables, a las instalaciones del RENIEC".

7.1.19.3. De ser el caso, el responsable del órgano o unidad orgánica debe solicitar a la OTI, la asignación de accesos lógicos

para las labores del tercero, siendo su responsabilidad informar el sustento de estos.

7.1.20. Abordar la seguridad de la información en los acuerdos con los proveedores (ISO 27001 A.5.20)

7.1.20.1. La OAF/ULG, debe incluir en los términos de referencia según sea el caso de servicios o bienes, respectivamente, el Anexo N°01 “Acuerdo de Confidencialidad” de la presente directiva, a fin de proteger los activos de información y los datos personales, a los cuales tendrán acceso los proveedores en el RENIEC; que se necesiten en coordinación, con el órgano o unidad orgánica.

7.1.20.2. Los Dueños del Proceso, Órganos y Unidades Orgánicas del RENIEC, deben definir en los términos de referencia los requisitos de seguridad de la información para asegurar que no haya malentendidos entre la organización y el proveedor respecto a las obligaciones de ambas partes, para lo cual podrá coordinar con el OSCD.

7.1.21. Gestión de la seguridad de la información en la cadena de suministro de las tecnologías de la información y la comunicación (TIC) (ISO 27001 A.5.21)

7.1.21.1. La OTI a través de sus unidades, y en coordinación con el OSCD deben identificar los requisitos de seguridad de la información para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios TIC, tales como:

a. Incluir parámetros de seguridad de información o Acuerdo de Nivel de Servicio dentro del contrato establecido y contemplar penalidades ante el incumplimiento, el nivel de servicio de los terceros debe ser evaluado y aceptado por los proveedores que entregan servicios de tecnologías de información, según su criticidad e impacto en la continuidad del negocio.

b. Los equipos de TIC al ser adquiridos tienen que ser revisados y contar con el visto bueno de la OTI. Asimismo, deben contar con garantía, mantenimiento preventivo y soporte técnico.

c. Verificar que el proveedor haya firmado Anexo N° 01 Acuerdo de Confidencialidad de la presente directiva.

d. Para la asignación y retiro de accesos para las labores del tercero, se debe se cumplir con el documento normativo "Solicitud de creación, activación, desactivación y cambio de nivel de usuarios", por parte del usuario que realiza la contratación del tercero.

7.1.22. Seguimiento, revisión y gestión de cambios en servicios de proveedores (ISO 27001 A.5.22)

7.1.22.1. El responsable del órgano o unidad orgánica del servicio debe (área usuaria):

a. Monitorear y revisar de acuerdo con lo especificado en los términos de referencia, en la orden de servicio y/o en el contrato del servicio del tercero, lo referido a seguridad de la información.
b. Revisar los informes producidos por el proveedor y organizar reuniones regulares de progreso según lo requieran los requisitos de seguridad de la información.
c. Comunicar las fallas e incidentes de seguridad de la información en los servicios de terceros.
d. Asegurar que el proveedor mantenga suficiente capacidad de servicio junto con planes viables diseñados para asegurar que los niveles de continuidad del servicio acordados se mantengan después de fallas importantes en el servicio o desastres.
e. Registrar todos los cambios y mejoras realizadas en los sistemas de comunicaciones u operaciones por servicios externos según la normatividad de contrataciones.

7.1.23. Seguridad de la información en el uso de servicios en la nube (ISO 27001 A.5.23)

7.1.23.1. La OTI administra el uso de servicios en la nube, teniendo en consideración lo siguiente:

a. Definir el alcance del servicio en la nube, además de las funciones y responsabilidades relacionadas con el uso y la gestión.
b. Establecer los controles de seguridad de la información que gestiona el proveedor de servicios en la nube y cuales gestiona la organización como cliente del servicio.

7.1.23.2. La SGTD detalla los lineamientos[13] para el uso de servicios en la nube para entidades de la Administración Pública del Estado Peruano, los cuales son:

a. Contar con una política de seguridad de la información, controles de Seguridad de la Información, proceso de gestión de riesgos.
b. Contar con una guía de buenas prácticas señaladas en la Directiva de Seguridad en el ámbito de la protección de datos personales.
c. Disponer de un Acuerdo de Nivel de Servicio - ANS con el proveedor de servicios en la nube, en la que quede claramente definida las responsabilidades de la entidad pública y el proveedor de servicios en la nube.
d. Requerir mínimamente al proveedor de servicios en la nube un certificado de seguridad de la información ampliamente reconocido y basado en estándares internacionales, el mismo que tiene que ser emitido por una organización de auditoría independiente.

[13] Resolución de Secretaría de Gobierno Digital N° 001-2018-PCM/SEGDI.

7.1.24. Planificación y preparación de la gestión de incidentes de seguridad de la información (ISO 27001 A.5.24)

7.1.24.1. En el documento normativo "Gestión de Incidentes de Seguridad de la Información" se detallan las pautas para tratar la planificación y preparación de la Gestión de incidentes de Seguridad de la Información.

7.1.25. Evaluación y decisión sobre eventos de seguridad de la información (ISO 27001 A.5.25)

7.1.25.1. Los riesgos e incidentes de seguridad de la información incluyen los riesgos e incidentes de seguridad digital. Asimismo, su gestión comprende una adecuada articulación entre el Oficial de Seguridad y Confianza Digital y los dueños de procesos, propietarios de riesgos, la máxima autoridad administrativa y el Titular de la entidad[14].

7.1.26. Respuesta a incidentes de seguridad de la información (ISO 27001 A.5.26), Aprendizaje de los incidentes de seguridad de la información (ISO 27001 A.5.27), Recolección de evidencia (ISO 27001 A.5.28)

7.1.26.1. La respuesta a los incidentes de Seguridad de la Información debe atenderse según lo definido en el documento normativo “Gestión de Incidentes de Seguridad de la Información”.

7.1.27. Seguridad de la información durante una interrupción (ISO 27001 A.5.29)

7.1.27.1. Los Dueños del proceso, órganos y unidades orgánicas del RENIEC son responsables de coordinar con el OSCD, los requisitos de seguridad de la información que se deben mantener y aquellos que por requerimiento de la operación deben ser suspendidos, ante una disrupción que ponga en peligro el desarrollo normal de las operaciones.

7.1.27.2. Los controles de seguridad de la información existentes en los diferentes procesos deben mantenerse durante la interrupción; caso contrario, se debe implementar controles de compensación.

7.1.27.3. Para tener evidencia de los controles que se aplican durante una disrupción se debe mantener en archivos las evidencias a través de diferentes medios entre las partes involucradas.

7.1.27.4. Al terminar la interrupción, los Dueños del proceso, órganos y unidades orgánicas del RENIEC que implementaron controles de compensación deben volver a implementar los controles iniciales debiendo informar al OSCD.

[14] Inciso 8.2 del Artículo 8. Responsables en la gestión de la seguridad digital institucional de la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD.

7.1.28. Preparación de las TIC para la continuidad del negocio (ISO 27001 A.5.30)

7.1.28.1. La OTI/UIST, establece el Plan de Recuperación de Desastres (DRP) en la parte tecnológica incluido en el Plan de Continuidad Operativa del RENIEC.

7.1.28.2. Para el desarrollo del Plan de Recuperación de Desastres en la parte tecnológica tomando como referencia lo descrito en la NTP/ISO 27002, se debe tener en cuenta lo siguiente:

a. El análisis de impacto al negocio (AIN), para determinar y evaluar los efectos potenciales de una interrupción operativa en el RENIEC como resultado de un desastre, accidente o emergencia.

b. El Tiempo Objetivo de Recuperación, que se refiere al tiempo máximo que el RENIEC requiere para recuperar sus procesos críticos, después de haber sido afectado por alguna contingencia (RTO) de cada servicio TIC priorizado y los procedimientos para restaurar esos componentes, evitando así el incumplimiento a los plazos establecidos en la normatividad vigente y aplicable al RENIEC.

c. El tiempo para determinar la pérdida de datos que se puede tolerar desde la última copia de seguridad creada (RPO) de los recursos TIC priorizados y los procedimientos para restaurar la información.

7.1.29. Requisitos legales, estatutarios, regulatorios y contractuales (ISO 27001 A.5.31)

7.1.29.1. La OAJ, es el órgano de asesoramiento encargado de brindar asesoría y asistencia técnica de carácter jurídico a la Alta Dirección y a los diferentes órganos y unidades orgánicas de la institución como órgano especializado en materia legal; así como analizar las normas, jurisprudencia, opiniones legales y doctrina jurídica relacionadas al quehacer de la institución.

7.1.29.2. El OSCD, debe llevar un registro de la lista maestra de documentos del Sistema de Gestión de Seguridad de la Información, el mismo que incluye la normativa emitida por la SGTD, en su calidad de ente rector en materia de Confianza Digital**.**

7.1.30. Derechos de propiedad intelectual (ISO 27001 A.5.32)

7.1.30.1. Los derechos de propiedad intelectual incluyen derechos de autor de software o documentos, derechos de diseños, y licencias de código fuente.

7.1.30.2. La OTI/UIS, debe proteger todo lo que se considere propiedad intelectual, según lo detallado a continuación:

a. La adquisición de software solo deberá realizarse a través de fuentes conocidas y acreditadas.

b. Conservar evidencias de propiedad de licencias, manuales, entre otros.

c. La OTI/UIST debe asegurar de que no se exceda el número máximo de usuarios o recursos permitido dentro de la licencia.

d. La OTI/UIST, realiza verificaciones para garantizar que solo se instalen software autorizado por la OTI y productos con licencia.

e. No duplicar, convertir a otro formato o extraer el código fuente que no sea lo permitido por la ley de derechos de autor o las licencias aplicables.

7.1.30.3. Es responsabilidad del órgano o unidad orgánica solicitar las licencias que necesitan para el desarrollo de sus actividades.

7.1.30.4. La instalación de software en los ambientes de procesamiento y/o estación de trabajo solo puede ser llevada a cabo por personal autorizado o por los mecanismos automáticos destinados a dicho fin.

7.1.30.5. La OTI/UIST, elabora y mantiene actualizado el inventario del software instalado en los equipos del servidor civil del RENIEC. En aquellos casos en que se detecten anomalías o licencias sin regularizar, la OTI/UIST informa al responsable del órgano o unidad orgánica involucrada y al OSCD, quienes comunican a la OPH/ USTPAD, para las investigaciones administrativas correspondientes y el deslinde de responsabilidades.

7.1.30.6. La OTI/UIS, define pautas para la administración y uso del software, mediante el documento normativo de “Administración de Software” con el propósito de asegurar la legalidad del software, el uso en cumplimiento de los términos de licencia correspondiente y la administración de los aplicativos desarrollados por la OTI/UIS o por terceros que brindan soporte institucional, toda vez que esta es propietaria del aplicativo y de los programas fuentes.

7.1.31. Protección de los registros (ISO 27001 A.5.33)

7.1.31.1. Es responsabilidad de la OGD, a través del Programa del Control de Documentos Archivísticos (PCDA), mantener el cronograma de retención de registros, donde considera los plazos establecidos por las entidades reguladoras a nivel nacional, los cuales deben ser revisados y actualizados cuando ocurran cambios en la normativa legal correspondiente, para garantizar que se mantiene vigente el esquema de clasificación y los requerimientos legales.

7.1.31.2. Los registros no deben ser destruidos antes de culminado el periodo de retención establecido en el Programa del Control de Documentos Archivísticos (PCDA).

7.1.31.3. Los registros de la entidad, incluyendo expedientes y documentos electrónicos deben ser protegidos y

mantenidos adecuadamente, por los dueños del proceso, órganos y unidades orgánicas del RENIEC

7.1.32. Privacidad y protección de la información de identificación personal (ISO 27001 A.5.34)

7.1.32.1. El OPDP es el encargado de informar y/o asesorar al RENIEC sobre las disposiciones de protección de datos personales, para la adopción de las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales, quien debe:

a. Proponer la incorporación de cláusulas en los documentos normativos para la suscripción de "Convenios de Suministro de Información con el RENIEC", enmarcados dentro de la Ley de Protección de Datos Personales.

b. Coordinar con los dueños del proceso, órganos y unidades orgánicas del RENIEC, la adopción de medidas de seguridad, técnicas, organizacionales y legales con el fin de velar por el cumplimiento de las normas en materia de protección de datos personales.

c. Reportar a la Autoridad Nacional de Protección de Datos Personales los incidentes de seguridad que impliquen la vulneración de la privacidad y protección de la información de identificación personal.

7.1.32.2. En cumplimiento de la Ley de Protección de Datos Personales, la Información de Identificación Personal (IIP) y la preservación de la privacidad es protegida en concordancia a las leyes, reglamentos aplicables. En tal sentido se dispone[15].

a. La adopción de Políticas de acuerdo con lo dispuesto por la Ley de Protección de Datos Personales.

7.1.33. Revisión independiente de la seguridad de la información (ISO 27001 A.5.35)

7.1.33.1. El enfoque aplicado por la organización para gestionar la seguridad de la información y su implementación incluida las personas, procesos y tecnologías debe revisarse de forma independiente en intervalos planificados o cuando se produzcan cambios significativos, para lo cual el OSCD en coordinación con los analistas de OTI/UGTI deben realizar el seguimiento y medición de los controles de seguridad de la información, según el plan de trabajo elaborado por la OTI/UGTI.

7.1.33.2. La OPPM/UMO gestiona el Programa Anual de Auditorías y evaluaciones internas de los Sistemas de Gestión del RENIEC; el cual debe revisarse de forma periódica o cuando se produzcan cambios significativos.

[15] Ley 29733 Ley de Protección de Datos Personales.

7.1.34. Cumplimiento con políticas, reglas y normas de seguridad de la información (ISO 27001 A.5.36)

7.1.34.1. SGEN a través del OSCD debe:

a. Coordinar la revisión periódica de las políticas de seguridad de la información del RENIEC, de los documentos normativos y los estándares correspondientes con la OTI/UGTI y órganos y unidades orgánicas involucradas.

b. Evaluar la necesidad de acciones correctivas y su implementación. Asimismo, registra y mantiene las evidencias de los resultados de las revisiones y acciones correctivas.

7.1.34.2. Los Dueños del proceso, órganos y unidades orgánicas del RENIEC, deben verificar el cumplimiento de la política de seguridad de la información de la institución e informar al OSCD cualquier incumplimiento por parte del/la servidor/a bajo su cargo.

7.1.35. Procedimientos operativos documentados (ISO 27001 A.5.37)

7.1.35.1 La OTI/UGTI coordina con los Dueños del proceso, órganos y unidades orgánicas involucradas relacionada con el SGSI del RENIEC (proceso de arranque y apagado de los servidores informáticos, respaldo, mantenimiento de equipos, seguridad y manejo del correo institucional, entre otros).

7.1.35.2 Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.

7.1.35.3 La información documentada debe estar disponible en la extensión necesaria para tener confianza en que los procesos se lleven a cabo según lo planificado.

7.1.35.4 Los Dueños del proceso, órganos y unidades orgánicas del RENIEC son responsables de asegurar la publicación de sus procedimientos, así como de llevar el ordenamiento, control y custodia de los mismos.

7.1.35.5 La publicación de los procedimientos se efectúa a través del INTRANET, de libre acceso a todo el personal de los diversos órganos y unidades orgánicas del RENIEC.

7.1.35.6 La difusión de los procedimientos se efectúa a través del Sistema Integrado de Trámite Documentario - SITD, mediante Memorando Múltiple por la OPPM dirigido a los diversos órganos del RENIEC, los cuales deben desplegar comunicación a sus respectivas unidades orgánicas y estos a su vez a todo el personal bajo su cargo.

7.1.36. Seguridad para el acceso a la información de Consultas RENIEC

Se debe implementar las siguientes medidas de protección para el acceso a la información de terceros al RENIEC a través del servicio de suministro de información por convenio de acuerdo al documento normativo “Convenios de Suministros de Información suscritos por el RENIEC”, Resolución Secretarial N° 000049-2023-SGEN_RENIEC y el acceso a consultas por la Plataforma Nacional de Interoperabilidad del Estado (PIDE):

Del RENIEC

7.1.36.1 La DCSD, debe:

a. Suspender el servicio del convenio con reconocimiento de costos a la empresa cuando se detecte la no actualización (bajas) de los usuarios finales, suspensión que queda sin efecto una vez subsanada dicha situación, procediendo a la reactivación del servicio.

b. Desactivar el acceso a todos aquellos usuarios finales que no hayan realizado uso de las consultas durante un plazo máximo de 30 días, siendo el coordinador de la entidad, el responsable de realizar nuevamente la habilitación del usuario.

7.1.36.2 En caso la DCSD o el OPDP tome conocimiento a través de cualquier medio de comunicación, del acceso indebido, mal uso de las consultas, entre otros, que pongan en riesgo la confidencialidad de la información de los ciudadanos, debe solicitar al responsable de convenios la desactivación del usuario final en forma inmediata; el RENIEC se encuentra facultado a realizar las comunicaciones correspondientes ante las autoridades pertinentes; a fin de realizar acciones administrativas o legales que correspondan según sea el caso, en cumplimiento de la Ley de Protección de Datos Personales.

7.1.36.3 Los convenios y similares que suscriba el RENIEC, deben incluir el “Cumplimiento de la política y objetivos de seguridad de la información” y “Cumplimiento de la ley N.° 29733, Ley de Protección de Datos Personales”, por lo que los usuarios se obligan a adoptar las medidas de seguridad y protección de la información; en caso de incumplimiento del convenio el RENIEC establece las acciones que considere conveniente.

7.1.36.4 El RENIEC, como custodio de la información del RUIPN está facultado para identificar e implementar todos aquellos controles que coadyuven a proteger la información del registro antes mencionado, por lo tanto, la DCSD, hará llegar hace llegar a las entidades públicas, personas jurídicas de derecho privado y notarios; controles de seguridad de la información, producto de la mejora continua de sus procesos, los cuales deben ser considerados como

parte integrante del convenio, o de los documentos normativos que serán de cumplimiento obligatorio.

7.1.36.5 Informar mediante cartas u oficios dirigidos a los titulares de las entidades públicas y privadas, sobre los controles de seguridad de la información, las mismas que son de cumplimiento obligatorio, y son coordinadas entre el OSCD, OPDP y órganos involucrados.

7.1.36.6 Para el caso de los servicios que se brindan por medio de la Plataforma de interoperabilidad PIDE, la DCSD para establecer las coordinaciones necesarias con la PCM, a fin de establecer en conjunto las acciones e implementaciones tecnológicas que de común acuerdo se ejecuten en bien de contribuir a la seguridad de la información y de los medios tecnológicos utilizados en dicha plataforma para efectos de brindar el servicio que proporciona el RENIEC.

De la Entidad

7.1.36.7 El Titular de la entidad que hace uso de las consultas a través de los servicios proporcionados por el RENIEC, es responsable de:

a. Mantener el registro de altas y bajas de sus usuarios finales, así como supervisar y controlar en forma integral y permanente el servicio de consultas, debiendo definir el mecanismo necesario para identificar quien consulto la información de un DNI, el RENIEC en cualquier momento que requiera solicitar la relación de usuarios finales habilitados; asimismo, el titular de la entidad se encuentra obligado de remitir en un plazo máximo de 7 días hábiles la relación en el que deben informar si los usuarios finales hacen uso de las consultas conforme las funciones asignadas.

b. Garantizar que dentro de su institución no se almacene información para construir una base de datos de las consultas realizadas por sus usuarios finales.

c. Brindar los controles necesarios para evitar los riesgos de seguridad de la información, para lo cual debe realizar un análisis de vulnerabilidad en forma semestral a dichas aplicaciones y remitir el informe y de ser el caso el plan de tratamiento al RENIEC para evidenciar el cumplimiento de este control.

d. Haber cumplido con los expresado en la Declaración Jurada de Seguridad de la Información y Protección de Datos Personales, el cual se consigna en la solicitud de suscripción de los servicios de suministro de información.

e. La obligación de cumplir las responsabilidades requeridas en el kit de sensibilización para las instituciones sobre el uso de los datos personales.

Del usuario final de la Entidad

7.1.36.8 El usuario final debe de manera expresa, sin excepción alguna, guardar estricta reserva de toda la información que el RENIEC le suministre a través de las consultas.

7.1.36.9 El usuario no cuenta con autorización alguna para grabar, almacenar, distribuir, transferir electrónicamente, vender o entregar gratuitamente a terceros, entre otras modalidades la información que el RENIEC le brinda; los datos brindados a los usuarios deben ser utilizados únicamente según los términos establecidos con el RENIEC.

7.1.36.10 La entidad es responsable de la alta y baja de usuarios finales, siendo requisito importante la baja de usuarios finales cuando ya no lo requieran para el cumplimiento de sus funciones, como rotación, cese, entre otros, bajo responsabilidad.

7.1.36.11 Para el caso de la PIDE las contraseñas deben tener un mínimo de 8 caracteres alfanuméricos y no contraseñas consecutivas; Los usuarios creados por primera vez y aquellos que hayan solicitado el reseteo de la contraseña deben en un plazo máximo de 01 día hábil ingresar a los servicios de consultas y realizar el cambio de la clave de acceso; en caso no cumpla con este requisito dentro del plazo establecido la OTI del RENIEC procederá a deshabilitarlo de oficio.

7.1.36.12 El usuario final no podrá tener acceso en diferentes entidades, estos solo podrán tener acceso a los servicios de suministro de información a través de una sola entidad, por lo cual, en caso de corroborarse esta acción se prohibirá el acceso hasta a la regularización.

Para el caso de los convenios

7.1.36.13 Todos los usuarios finales de convenios que realicen consultas y otras bases de datos del RENIEC deben acceder y realizar las consultas con su DNIe.

7.1.36.14 Las responsabilidades para el proceso de suministro de información son definidas en el lineamiento “Sobre convenios de suministro de información suscritos por el RENIEC”.

7.1.36.15 En el caso de los convenios ya suscritos, se aplica lo establecido en el documento normativo “Convenios de Suministro de Información suscritos por el RENIEC” según corresponda.

7.1.36.16 La DCSD, dentro de su facultad supervisora y de control, procede a:

a. Evaluar el uso que da el Usuario respecto a la información suministrada por el RENIEC de acuerdo con los convenios o a través de la PIDE, la cual debe encontrarse acorde a lo declarado por el mismo en su solicitud. En el supuesto caso de advertir un uso inadecuado del servicio o el incumplimiento de las cláusulas del convenio o controles de seguridad de la información, en coordinación con la OTI, se encuentra facultada a realizar una inspección a la entidad o persona jurídica de derecho privado o público, a efecto de verificar el uso de la información de identificación suministrada a través de los servicios de consultas en línea.

b. Suspender el servicio a la entidad cuando se detecte alguna incongruencia de los datos declarados o la no actualización, supuesto uso inadecuado del servicio o el incumplimiento de las cláusulas del convenio de suministro de información por parte de los usuarios finales.

c. Resolver el convenio y desactivar los servicios de la entidad, en caso de detectar observaciones en la supervisión que realice a la entidad, relativas al uso indebido del servicio o incumplimiento de las cláusulas del convenio, sin perjuicio de que se inicie las acciones penales que correspondan.

d. Denegar plenamente el acceso al servicio de suministro de información al usuario y/o usuario final que haya realizado un uso inadecuado del servicio o el incumplimiento de las cláusulas del convenio de suministro de información.

e. Desactivar el servicio de suministro de información y resolver el convenio en caso se mantenga un saldo pendiente en los últimos tres (03) meses.

f. Deshabilitar el acceso al usuario final del servicio de suministro de información en caso no haya hecho uso del servicio a través de consultas en los últimos treinta (30) días.

g. Eliminar el acceso al usuario final del servicio de suministro de información en caso no haya hecho uso del servicio a través de consultas en los últimos sesenta (60) días.

h. En caso la entidad no haya realizado consultas en los últimos noventa (90) días, la DCSD está facultada a efectuar el apartamiento o resolución del convenio, para tal efecto, se enviará un oficio comunicando el

apartamiento del convenio.

VIII. DISPOSICIÓN COMPLEMENTARIA

8.1 Cualquier situación no contemplada en la presente Directiva, respecto a la seguridad de la información del RENIEC, debe ser informada por los Dueños de los procesos, gestor de seguridad de la información y servidor civil, a la OSCD para la gestión correspondiente.

8.2 La OTI a través de sus Unidades Orgánicas, informa cualquier evento o incidente que resulte pertinente al OSCD, a fin de contribuir con la implementación mantenimiento del SGSI del RENIEC y sea solucionado e informado oportunamente.

8.3 En caso de incumplimiento por parte del funcionario/a o servidor/a civil 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.

XI. ANEXOS

Anexo N° 01 _ Acuerdo de Confidencialidad

Este Acuerdo de Confidencialidad entre EL RENIEC y EL CONTRATISTA/PROVEEDOR **……., en adelante denominado (EL TERCERO).**

1) **EL TERCERO** se compromete a respetar y aplicar en la ejecución de las labores del presente contrato/orden de servicio, las políticas, los procedimientos, los estándares y los controles de seguridad de la información establecidos por EL RENIEC, los mismos que declara conocer y aceptar.
2) **EL TERCERO** deberá proteger los activos de información (información, software, hardware físicos, documentación, entre otros) EL RENIEC de acceso no autorizado, pérdida, modificación y/o destrucción, falsificación, robo, uso Indebido y/o divulgación no autorizada.
3) **EL TERCERO** se obliga a mantener y guardar estricta reserva y absoluta confidencialidad de todos los documentos o informaciones de **EL RENIEC** a los que tenga acceso en ejecución del presente contrato/orden de servicio. Se entiende que la obligación asumida por **EL TERCERO** está referida no solo a los documentos e informaciones señalados como "confidenciales" sino a todos los documentos o informaciones que debido al presente contrato/orden de servicio o vinculado con la ejecución del mismo pueda ser conocida por cualquier medio por **EL TERCERO**.
4) En consecuencia, **EL TERCERO** deberá abstenerse de divulgar tales documentos, conversaciones, acuerdos de reuniones y comentarios que como parte de la función son de uso conocimiento, sea en forma directa o indirecta.
5) **EL TERCERO** solo podrá revelar al personal que estrictamente sea necesario para la realización de las actividades materia del presente contrato/orden de servicio, los documentos e informaciones a los que se refiere el numeral precedente.
6) En el caso que **EL TERCERO** fuera requerido (a) por alguna autoridad administrativa o judicial para revelar la información y/o documentación a la que se refiere la presente cláusula, **EL TERCERO** deberá notificar anticipadamente a **EL RENIEC** para que esta adopte las medidas que considere necesarias para proteger la confidencialidad de la información.
7) Se deja expresamente establecido que el deber de confidencialidad o suscripción del presente contrato/orden de servicio se extiende incluso hasta después del cese de la relación contractual con la organización por el lapso de 5 años).
8) **EL TERCERO** se compromete a devolver todo activo (software, documentación, equipos, claves de acceso, entre otros) que le haya proporcionado EL RENIEC para el desempeño de sus funciones al momento de resolución o término del presente contrato/orden de servicio, sin que sea necesario que éste se lo requiera.
9) El incumplimiento de las obligaciones que asume **EL TERCERO** en las cláusulas precedentes constituye la resolución del presente contrato/orden de servicio, de conformidad con lo previsto en el artículo 164° del Reglamento de la Ley N° 30225, Ley de Contrataciones del Estado, sin perjuicio de la obligación de **EL TERCERO** de pagar a EL RENIEC la indemnización correspondiente.
10) **EL TERCERO** debe llevar a cabo sus obligaciones bajo este Acuerdo usando las mismas normas de seguridad que utiliza para proteger su propia información, o por lo menos un razonable grado de seguridad, por lo cual el personal que presta el servicio debe conocer las siguientes **Conductas no aceptadas:**

- Todas aquellas indicadas en la Ley como figuras penales relativas a la informática (Ley de Delitos Informáticos, Ley N° 30096), derechos de autor (Decreto Legislativo N° 822) y a la ley de protección de datos personales (Ley N° 29733); algunos ejemplos de éstas:
  - ✓ Acceso o intromisión en sistemas para apoderarse, usar o conocer indebidamente la información contenida en él.
  - ✓ Daño o alteración de los datos contenidos en un sistema de información.
  - ✓ Inutilización de sistemas de información, sus partes o componentes, y/o la obstaculización en la prestación de los servicios.
  - ✓ Revelación o difusión de datos contenidos en un sistema.
  - ✓ Copiar o distribuir software, datos, códigos y manuales sin la expresa autorización.

- ✓ Usar copias no autorizadas del software (sin la debida licencia). Esto incluye la ejecución simultánea de software en dos o más computadores salvo que conste debidamente autorizado en la licencia de uso.
- ✓ Fabricar, adquirir o utilizar cualquier elemento que sirva para remover o burlar, aspectos de seguridad del software, servidores informáticos, equipos o de las redes.
- ✓ Utilizar los recursos, accesos a los sistemas o páginas web, a las que tenga acceso, para realizar otras actividades distintas a las enmarcadas dentro de mis funciones

Encontrándose las partes conformes con la ejecución de este Acuerdo, el representante autorizado de **EL TERCERO** procede a la suscripción.

En la ciudad de Lima, el _____de _____ del 20__.

_____

Este documento deberá ser incluido en todos los contratos que la institución formalice

Anexo N° 02 _ Contacto con grupos de interés especial del Sistema de Gestión de Seguridad de la Información

CONTACTO CON GRUPOS DE INTERÉS ESPECIAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Versión del Registro:	
Fecha de Actualización:	

N°	ENTIDAD O EMPRESA	DESCRIPCIÓN	CONTACTO	TELÉFONO	CORREO ELECTRONICO/PAGINA WEB	COMENTARIOS

Anexo N° 03 _ Cuadro de control de cambios

VERSIÓN VIGENTE (Listar los títulos/capítulos y numerales del DN)	REGISTRO DE CAMBIO (Descripción de los títulos/capítulos y numerales del DN)	ACCIÓN (Modificado, incluido, eliminado)
I. OBJETIVO	***OBJETIVO***	*Ninguno*
II. ALCANCE	***II. ALCANCE***	*Ninguno*
III. BASE LEGAL	***III. BASE LEGAL***	*Ninguno*
3.1 Párrafo vigente	*3.1 Párrafo vigente*	*Ninguno*
3.2 Párrafo vigente	*3.2 Párrafo vigente*	*Ninguno*
3.3 Párrafo vigente	*3.3 Párrafo vigente*	*Ninguno*
3.4 Párrafo vigente	*3.4 Párrafo vigente*	*Ninguno*
	3.5 Nuevo Párrafo ***Ley N° 27815,*** *Ley del Código de Ética de la Función Pública, del 22 de julio de 2002 y sus modificatorias*	*Incluido*
3.5 Párrafo vigente	*3.6 Párrafo vigente*	*Ninguno*
3.6 Párrafo vigente	*3.7 Párrafo vigente*	*Ninguno*
3.7 Párrafo vigente	*3.8 Párrafo vigente*	*Ninguno*
3.8 Párrafo vigente	*3.9 Párrafo vigente*	*Ninguno*
3.9 Párrafo vigente	*3.10 Párrafo vigente*	*Ninguno*
	3.11 Nuevo Párrafo ***Decreto Supremo N° 015-98-PCM****, Reglamento de las Inscripciones del Registro Nacional de Identificación y Estado Civil y sus modificatorias.*	*Incluido*
3.10 Párrafo vigente	*3.12 Párrafo vigente*	*Ninguno*
3.11 Párrafo vigente	*3.13 Párrafo vigente*	*Ninguno*
3.12 Párrafo vigente	*3.14 Párrafo vigente*	*Ninguno*
3.13 Párrafo vigente	*3.15 Párrafo vigente*	*Ninguno*
3.14 Párrafo vigente	*3.16 Párrafo vigente*	*Ninguno*
	3.17 Nuevo Párrafo ***Decreto Supremo N° 092-2017-PCM,*** *que aprueba la Política Nacional de Integridad y Lucha*	*Incluido*

	Contra la Corrupción, del 14 de setiembre de 2017.	
3.15 Párrafo vigente	*3.18 Párrafo vigente*	*Ninguno*
	3.19 Nuevo Párrafo ***Decreto Supremo N° 042-2018-PCM,** que establece medidas para Fortalecer la Integridad Pública y Lucha Contra la Corrupción del 22 de abril de 2018.*	*Incluido*
	3.20 Nuevo Párrafo ***Decreto Supremo N° 044-2018-PCM,** que aprueba el Plan Nacional de Integridad y Lucha Contra la Corrupción 2018-2021, del 26 de abril de 2018; mantiene su vigencia según lo dispuesto en el **Decreto Supremo N° 180-2021-PCM** del 10 de diciembre de 2021.*	*Incluido*
3.16 Párrafo vigente	*3.21 Párrafo vigente*	*Ninguno*
3.17 Párrafo vigente	*3.22 Párrafo vigente*	*Ninguno*
3.18 Párrafo vigente	*3.23 Párrafo vigente*	*Ninguno*
3.19 Párrafo vigente	*3.24 Párrafo vigente*	*Ninguno*
3.20 Párrafo vigente	*3.25 Párrafo vigente*	*Ninguno*
3.21 Párrafo vigente	*3.26 Párrafo vigente*	*Ninguno*
3.22 Párrafo vigente	*3.27 Párrafo vigente*	*Ninguno*
3.23 Párrafo vigente	*3.28 Párrafo vigente*	*Ninguno*
3.24 Párrafo vigente	*3.29 Párrafo vigente*	*Ninguno*
3.25 Párrafo vigente	*3.30 Párrafo vigente*	*Ninguno*
3.26 Párrafo vigente	*3.31 Párrafo vigente*	*Ninguno*
3.27 Párrafo vigente	*3.32 Párrafo vigente*	*Ninguno*
3.28 Párrafo vigente	*3.33 Párrafo vigente*	*Ninguno*
3.29 Párrafo vigente	*3.34 Párrafo vigente*	*Ninguno*
3.30 Párrafo vigente	*3.35 Párrafo vigente*	*Ninguno*
3.31 Párrafo vigente ***Resolución Jefatural Nº 000056-2024/JNAC/RENIEC,** que aprueba el Plan Estratégico Institucional (PEI) correspondiente al período 2021 -*	-	*Eliminado*

2027 Ampliado del Registro Nacional de Identificación y Estado Civil - RENIEC, del 29 de marzo de 2024.		
3.32 Párrafo vigente	*3.36 Párrafo vigente*	*Ninguno*
3.33 Párrafo vigente ***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.*	-	*Eliminado*
3.34 Párrafo vigente ***Resolución Secretarial N° 000004-2023/SGEN/RENIEC,*** *que aprueba la Directiva DI-010-OIR/002 "Gestión Integral del Riesgo", del 09 de enero de 2023.*	-	*Eliminado*
3.35 Párrafo vigente ***Resolución Secretarial N° 000059-2024/SGEN/RENIEC,*** *que aprueba el Manual de Clasificador de Cargos del Registro Nacional de Identificación y Estado Civil – RENIEC, del 12 de junio de 2024.*	-	*Eliminado*
3.36 Párrafo vigente	*3.37 Párrafo vigente*	*Ninguno*
3.37 Párrafo vigente	*3.38 Párrafo vigente*	*Ninguno*
3.38 Párrafo vigente	*3.39 Párrafo vigente*	*Ninguno*
IV. TÉRMINOS Y DEFINICIONES	***V. TÉRMINOS Y DEFINICIONES***	*Ninguno*
4.1 Párrafo vigente	*4.1 Párrafo vigente*	*Ninguno*
4.2 Párrafo vigente	*4.2 Párrafo vigente*	*Ninguno*
	4.3 Nuevo Párrafo ***Alta Dirección*** *Está conformado por la Jefatura Nacional, Gerencia General y Secretaría General.*	*Incluido*
4.3 Párrafo vigente ***Confidencialidad*** *Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.*	*4.4 Párrafo modificado* ***Confidencialidad*** *Propiedad de que la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.*	*Modificado*
4.4 Párrafo vigente	*4.5 Párrafo vigente*	*Ninguno*

4.5 Párrafo vigente ***Desclasificación*** *Es el acto de disponer con carácter con carácter público la información declarada con carácter secreto, reservado o confidencial mediante acto resolutivo.*	-	*Eliminado*
4.6 Párrafo vigente	*4.6 Párrafo vigente*	*Ninguno*
4.7 Párrafo vigente	*4.7 Párrafo vigente*	*Ninguno*
4.8 Párrafo vigente	*4.8 Párrafo vigente*	*Ninguno*
4.9 Párrafo vigente ***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.*	*4.9 Párrafo modificado* ***Incidente de Seguridad de la Información*** *Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de una organización o comprometer sus operaciones y amenazar la seguridad de la información de la entidad pública.*	*Modificado*
4.10 Párrafo vigente ***Propietario del Activo*** *El propietario de un activo de información puede ser un individuo o una entidad que a la que la dirección ha asignado la responsabilidad de gestionar el activo en su ciclo de vida completo.*	*4.10 Párrafo modificado* ***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.*	*Modificado*
4.11 Párrafo vigente ***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.*	*4.10 Párrafo modificado* ***Propietario del Activo*** *El propietario de un activo de información puede ser un individuo o una entidad que a la que la dirección ha asignado la responsabilidad de gestionar el activo en su ciclo de vida completo.*	*Modificado*
4.12 Párrafo vigente	*4.12 Párrafo vigente*	*Ninguno*
4.13 Párrafo vigente	*4.13 Párrafo vigente*	*Ninguno*
4.14 Párrafo vigente	*4.14 Párrafo vigente*	*Ninguno*
4.15 Párrafo vigente	*4.15 Párrafo vigente*	*Ninguno*
4.16 Párrafo vigente ***Riesgos*** *Probabilidad que una amenaza se materialice, al producirse exposición a un a vulnerabilidad existente.*	*4.16 Párrafo modificado* ***Riesgo*** *Efecto de la incertidumbre sobre los objetivos.*	*Modificado*

4.17 Párrafo vigente	*4.17 Párrafo vigente*	*Ninguno*
4.18 Párrafo vigente	*4.18 Párrafo vigente*	*Ninguno*
4.19 Párrafo vigente ***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, de gestión del riesgo y mejora continua.*	*4.19 Párrafo modificado* ***Sistema de Gestión de Seguridad de la Información SGSI*** *Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para lograr los objetivos comerciales. Se basa en una evaluación de riesgos y los niveles de aceptación de riesgos de la organización diseñados para tratar y gestionar los riesgos de forma eficaz. Analizar los requisitos para la protección de los activos de información y aplicar controles adecuados para garantizar la protección de estos activos de información, según sea necesario, contribuye a la implementación exitosa de un SGSI; y consta de políticas, procedimientos, directrices, recursos y actividades asociados, gestionados colectivamente por una organización, en la búsqueda de proteger sus activos de información.*	*Modificado*
4.20 Párrafo vigente	*4.20 Párrafo vigente*	*Ninguno*
V. RESPONSABILIDADES *Párrafo vigente* *En función de los controles físicos de seguridad de la información del SGSI, se establecen las responsabilidades de los Dueños del proceso, órganos y unidades orgánicas involucradas.*	***V. RESPONSABILIDADES*** *Párrafo modificado* *En función de los controles organizacionales de seguridad de la información del SGSI, se establecen las responsabilidades de los Dueños del Proceso, órganos y unidades orgánicas involucradas, de acuerdo a las funciones conferidas en el ROF del RENIEC y normativa vigentes.*	*Modificado*
5.1 Párrafo vigente ***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.*	*5.1 Párrafo modificado* ***Jefatura Nacional JNAC*** *Es responsable de aprobar la política y objetivos de seguridad de la información del SGSI - RENIEC, mediante Resolución Jefatural.*	*Modificado*
	5.2 Nuevo Párrafo ***Gerencia General GG*** *Asegurar y monitorear la implementación, mantenimiento, desempeño y funcionamiento de los Sistemas de Gestión, así como el*	*Incluido*

	cumplimiento de sus procesos, procedimientos y actividades de los órganos y unidades orgánicas de línea.	
5.2 Párrafo vigente ***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.*	*5.3 Párrafo modificado* ***Secretaría General SGEN*** *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; así como de informar al Titular de la entidad los avances y dificultades en la implementación u operación del SGSI del RENIEC.*	*Modificado*
5.3 Párrafo vigente ***Oficina de Seguridad y Defensa Nacional OSDN*** Es responsabilidad de la OSDN, cumplir con los controles de seguridad física, en relación a la gestión del Sistema de Seguridad Institucional, que garantice la protección de las personas, los bienes, las instalaciones y el normal funcionamiento de los servicios de la institución, según lo descrito en el sub numeral 6.5 y detallado en el título VII. Disposiciones Específicas los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente Asimismo, se debe cumplir con los procesos normados en relación a la salida y/o desplazamiento de bienes muebles patrimoniales de carácter informático normados por la OAF.	*5.4 Párrafo modificado* ***Oficina de Seguridad y Defensa Nacional OSDN*** *Es responsable, de supervisar el cumplimiento de los controles relacionados con la gestión del sistema de seguridad institucional, que garantice la protección de las personas, los bienes, las instalaciones y el normal funcionamiento de los servicios de la institución; los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	*Modificado*
5.4 Párrafo vigente ***Oficina de Integridad y Lucha contra la Corrupción OILCC*** *Es responsabilidad de la OILCC, revisar y actualizar el marco normativo para la gestión del riesgo en la institución, según lo descrito en el sub numeral 6.6 y detallado en el título VII. Disposiciones Específicas los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente*	*5.5 Párrafo modificado* ***Oficina de Integridad y Lucha contra la Corrupción OILCC*** *Es responsable de coordinar con los diferentes órganos y unidades orgánicas de la institución la aplicación del marco normativo para la gestión del riesgo: identificación, análisis, valoración, tratamiento y seguimiento de los riesgos; así como revisar y actualizar de forma periódica el marco normativo correspondiente, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	*Modificado*
5.5 Párrafo vigente	*5.6 Párrafo modificado*	*Modificado*

Oficina de Planificación, Presupuesto y Modernización OPPM *Es responsabilidad de la OPPM, a través de la Unidad de Modernización Organizacional, orientar a la OSCD para asegurar una adecuada articulación con los instrumentos de gestión institucional comprendidos en los sistemas administrativos de presupuesto público, planeamiento estratégico, programación multianual y gestión de inversiones, según lo descrito en el sub numeral 6.7 y detallado en el título VII. Disposiciones Específicas los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	***Oficina de Planificación, Presupuesto y Modernización OPPM*** *Es responsable, a través de sus unidades adscritas (Unidad de Planeamiento e Inversiones, Unidad de Presupuesto y Unidad de Modernización Organizacional), orientar a la OSCD para asegurar una adecuada articulación de los instrumentos de gestión institucional, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	
5.6 Párrafo vigente **Oficina de Asesoría Jurídica OAJ** *Es responsabilidad de la OAJ cumplir con los controles de seguridad de la información, en relación a la asistencia técnica de carácter jurídico, según lo descrito en el sub numeral 6.8 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 Párrafo modificado* ***Oficina de Asesoría Jurídica OAJ*** *Es responsable de cumplir con los controles de seguridad de la información, relacionados a la asistencia técnica de carácter jurídico, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	*Modificado*
5.7 Párrafo vigente ***Oficina de Administración y Finanzas OAF*** *Es responsabilidad de la OAF, normar, según las disposiciones legales establecidas dentro del Sistema Nacional de Abastecimiento, el proceso de salida de la entidad de los bienes muebles patrimoniales de naturaleza informática, los cuales se realizarían por motivos de teletrabajo, desplazamientos externos por diversas causas, entre otros relacionados y afines solo a usos institucionales; así como normar las responsabilidades de los usuarios, indicándoles las responsabilidades por el indebido uso de los equipos informáticos de la entidad, a efecto de que se lleve un adecuado control a través de la Unidad de Servicios Generales y Control Patrimonial, según lo descrito en el sub numeral 6.9 y detallado en el título VII. Disposiciones Específicas los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	*5.8 Párrafo modificado* ***Oficina de Administración y Finanzas OAF*** *Es responsable de normar, según el marco legal vigente dentro del Sistema Nacional de Abastecimiento, el proceso de salida de la entidad de los bienes muebles patrimoniales de naturaleza informática, los cuales se realizan por motivos de teletrabajo, desplazamientos externos por diversas causas, entre otros relacionados y afines solo para uso institucional; así como normar las responsabilidades de los usuarios, dando lineamientos sobre el debido uso de los equipos informáticos de la entidad, a efecto de que se lleve un adecuado control a través de la Unidad de Servicios Generales y Control Patrimonial, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	*Modificado*

5.8 Párrafo vigente ***Oficina de Potencial Humano OPH*** *Es responsabilidad de la OPH, cumplir con los controles de seguridad de la información, en relación a la gestión del recurso humano de la institución, según lo descrito en el sub numeral 6.10 y detallado en el título VII. Disposiciones Específicas los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	*5.9 Párrafo modificado* ***Oficina de Potencial Humano OPH*** *Es responsable de gestionar el recurso humano de la institución, en relación a la capacitación, seguridad y salud en el trabajo; así como gestionar los procesos administrativos disciplinarios, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	*Modificado*
	5.10 Nuevo Párrafo ***Oficina de Comunicaciones y Prensa*** *Es responsable de supervisar y evaluar las políticas y estrategias de la gestión de comunicación institucional, comunicación digital, prensa, publicidad, protocolo, relaciones institucionales y acciones de responsabilidad social; velando por la identidad, la imagen y la reputación de la institución, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	*Incluido*
	5.11 Nuevo Párrafo ***Oficina de Tecnologías de la Información OTI*** *Es responsable, a través de sus unidades adscritas (Unidad de Infraestructura y Soporte Tecnológico, Unidad de Gobierno de Tecnologías de la Información, y Unidad de Ingeniería de Software) del soporte tecnológico de la institución a nivel nacional e internacional, encargada de brindar servicios de tecnología de la información y comunicación oportuna y veraz, promoviendo el uso ético de las tecnologías digitales; así como de informar al Oficial de Seguridad y Confianza Digital (OSCD) todo incidente de seguridad digital crítico que afecte los procesos misionales y servicios que brinda la entidad, de forma inmediata. Asimismo, articula con el OSCD la implementación de controles de seguridad de la información y coordina con el Equipo de Respuestas ante Incidentes de Seguridad Digital la gestión de incidentes de seguridad digital.*	*Incluido*

5.9 Párrafo vigente ***Unidad de la Infraestructura y Soporte Tecnológico UIST*** *Es responsabilidad de la UIST, cumplir con los controles de seguridad de la información, en relación a los servicios informáticos internos y externos, funcionamiento de la base de datos y redes de comunicaciones, según lo descrito en el sub numeral 6.11 y detallado en el título VII. Disposiciones Específicas los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	*5.12 Párrafo modificado* ***Unidad de Infraestructura y Soporte Tecnológico UIST*** *Es responsable de cumplir con los controles de seguridad de la información, con relación a los servicios informáticos internos y externos, funcionamiento de la base de datos y redes de comunicaciones, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	*Modificado*
	5.13 Nuevo Párrafo ***Unidad de Gobierno de Tecnologías de la Información UGTI*** *Es responsable, de coordinar las acciones de implementación y mantenimiento de controles de seguridad digital en el marco del Sistema de Gestión de Seguridad de la Información – SGSI, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	*Incluido*
5.10 Párrafo vigente ***Unidad de ingeniería de Software UIS*** *Es responsabilidad de la UIS, cumplir con los controles de seguridad de la información, en relación a la planificación y desarrollo de los sistemas informáticos, según lo descrito en el sub numeral 6.12 y detallado en el título VII. Disposiciones Específicas los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	*5.14 Párrafo modificado* ***Unidad de Ingeniería de Software UIS*** *Es responsable de cumplir con los controles de seguridad de la información, relacionados a la planificación y desarrollo de los sistemas informáticos, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	*Modificado*
5.11 Párrafo vigente ***Oficina de Gestión Documental OGD*** *Es responsabilidad de la OGD, cumplir con los controles de seguridad de la información, en relación a la administración del modelo de gestión documental de la institución, según lo descrito en el sub numeral 6.13 y detallado en el título VII. Disposiciones Específicas los que obedecen a las funciones conferidas*	*5.15 Párrafo modificado* ***Oficina de Gestión Documental OGD*** *Es responsable de cumplir con los controles de seguridad de la información, relacionados con la administración del modelo de gestión documental de la institución, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	*Modificado*

en el ROF del RENIEC y normativa vigente.		
5.12 Párrafo vigente ***Dirección de Certificación y Servicios Digitales DCSD*** *Es responsabilidad de la DSCD, cumplir con los controles de seguridad de la información, con relación a la Seguridad para el acceso a la información de Consultas RENIEC. según lo descrito en el sub numeral 6.14 y detallado en el título VII. Disposiciones Específicas los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	*5.16 Párrafo modificado* ***Dirección de Certificación y Servicios Digitales DCSD*** *Es responsable de cumplir con los controles de seguridad de la información, relacionados a la seguridad para el acceso a la información de Consultas RENIEC, los que obedecen a las funciones conferidas en el ROF del RENIEC y normativa vigente.*	*Modificado*
5.13 Párrafo vigente ***Secretaria de Gobierno y Transformación Digital SGTD*** *La Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros (PCM) lidera la articulación, implementación y evaluación de la Política Nacional de Transformación Digital y su estrategia, así como las políticas nacionales, planes nacionales, normas, lineamientos, proyectos y plataformas para tal fin.*	-	*Eliminado*
	5.17 Nuevo Párrafo ***Oficial de Protección de Datos Personales OPDP*** *El ODP interviene como enlace con la Autoridad Nacional de Protección de Datos Personales (ANPD), coopera y efectúa seguimiento a los lineamientos y directivas que emita dicha Autoridad, así como aquellos establecidos en el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital; y dispone medidas para su fortalecimiento.*	*Incluido*
5.14 Párrafo vigente	*5.18 Párrafo vigente*	*Ninguno*
5.14.1 Párrafo vigente	*5.18.1 Párrafo vigente*	*Ninguno*
5.14.2 Párrafo vigente	*5.18.2 Párrafo vigente*	*Ninguno*
5.14.3 Párrafo vigente *Formular y actualizar la presente Directiva y procedimientos en materia de Seguridad de la Información*	*5.18.3 Párrafo modificado* *Formular y actualizar la presente Directiva y procedimientos en materia*	*Modificado*

acorde a lo dispuesto en la Directiva DI-001-OPPM/001 "Documentos Normativos del RENIEC".	*de Seguridad de la Información acorde a la normativa vigente.*	
5.14.4 Párrafo vigente	*5.18.4 Párrafo vigente*	*Ninguno*
5.15 Párrafo vigente ***Oficial de Protección de Datos Personales OPDP*** *El ODP actúa como enlace con la Autoridad Nacional de Protección de Datos Personales (ANPD), coopera y sigue los lineamientos y directivas que emita dicha Autoridad, así como aquellos establecidos en el Decreto de Urgencia Nº 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital; y, dispone medidas para su fortalecimiento.*	-	*Eliminado*
VI. DISPOSICIONES GENERALES	***VI. DISPOSICIONES GENERALES***	*Ninguno*
6.1 Párrafo vigente *La Jefatura Nacional es responsable de aprobar las políticas y objetivos de seguridad de la información.*	-	*Eliminado*
6.2 Párrafo vigente *La SGEN es el órgano formulador y quien administra las disposiciones de la presente Directiva.*	-	*Eliminado*
6.3 Párrafo vigente *Los Dueños del Proceso, Órganos y Unidades Orgánicas del RENIEC, conforme a sus funciones cuentan con facultades para definir o actualizar los controles organizacionales de seguridad de la información contenidos en la presente Directiva, en coordinación con la OSCD, OAF, OAJ, OPH, OPPM, OSDN, OGD, OILCC, OTI y OPDP.*	*6.1 Párrafo modificado* *Los Dueños del Proceso, órganos y unidades orgánicas del RENIEC, conforme a sus funciones cuentan con facultades para definir, proponer o actualizar los controles organizacionales de seguridad de la información contenidos en la presente Directiva, en coordinación con el OSCD, OPDP y con los OO. y UU. OO involucradas según corresponda.*	*Modificado*
6.4 Párrafo vigente *La OSDN gestiona los controles relacionados a control de acceso y seguridad de la información en las relaciones con los proveedores.*	*6.2 Párrafo modificado* *La OSDN gestiona el sistema de control de visitas - PCM y supervisa el servicio que brindan las empresas de seguridad y vigilancia en las instalaciones de la institución.*	*Modificado*

6.5 Párrafo vigente *La OILCC gestiona los documentos normativos para la clasificación de los activos de seguridad de la información.*	-	*Eliminado*
6.6 Párrafo vigente *La OPPM gestiona el control relacionado a revisión independiente de la seguridad de la información y Procedimientos operativos documentados.*	*6.3 Párrafo modificado* *La OPPM gestiona el control relacionado a los planes, programas y documentos de gestión interna de la institución.*	*Modificado*
6.7 Párrafo vigente	*6.4 Párrafo vigente*	*Ninguno*
6.8 Párrafo vigente	*6.5 Párrafo vigente*	*Ninguno*
6.9 Párrafo vigente *La OPH gestiona los controles relacionados a contacto con autoridades, Control de acceso y las acciones correspondientes a las investigaciones administrativas relacionadas al incumplimiento del control derechos de la propiedad intelectual.*	*6.6 Párrafo modificado* *La OPH gestiona el recurso humano de la institución, así como lo relacionado al Sistema de Gestión de la Seguridad y Salud en el Trabajo - SGSST, asegurando las condiciones de trabajo que garanticen la salud y seguridad ocupacional en coordinación con el Comité designado por la Alta Dirección.*	*Modificado*
6.10 Párrafo vigente	*6.7 Párrafo vigente*	*Ninguno*
6.11 Párrafo vigente *La OTI/UGTI gestiona los controles relacionados a revisión independiente de la seguridad de la información revisión independiente de la seguridad de la información.*	*6.8 Párrafo modificado* *La OTI/UGTI gestiona los controles relacionados a las acciones de implementación y mantenimiento de seguridad digital en el marco del Sistema de Gestión de Seguridad de la Información - SGSI.*	*Modificado*
6.12 Párrafo vigente	*6.9 Párrafo vigente*	*Ninguno*
6.13 Párrafo vigente	*6.10 Párrafo vigente*	*Ninguno*
6.14 Párrafo vigente	*6.11 Párrafo vigente*	*Ninguno*
6.15 Párrafo vigente *El OPDP gestiona el control relacionado a privacidad y protección de la información de identificación personal.*	*6.12 Párrafo modificado* *El OPDP gestiona el control relacionado a privacidad y protección de la información de identificación personal.*	*Modificado*
6.16 Párrafo vigente *La OSCD gestiona los controles relacionados a políticas para la seguridad de la Información, roles y responsabilidades en Seguridad de la*	*6.13 Párrafo modificado* *La OSCD gestiona los controles relacionados a políticas para la seguridad de la Información, roles y responsabilidades en seguridad de la*	*Modificado*

Información, contacto con grupos especiales de interés, inteligencia de amenazas, clasificación de la información, Abordar la seguridad de la información en los acuerdos con los proveedores, evaluación y decisión sobre eventos de seguridad de la información, requisitos legales, estatutarios, regulatorios y contractuales, Derechos de propiedad intelectual, revisión independiente de la seguridad de la información y cumplimiento con políticas, reglas y normas de seguridad de la información y Seguridad para el acceso a la información de Consultas RENIEC.	*información, contacto con grupos especiales de interés, inteligencia de amenazas, clasificación de la información; así como aborda la seguridad de la información en los acuerdos con los proveedores, evalúa en coordinación con los órganos y unidades responsables sobre los eventos de seguridad de la información, requisitos legales, estatutarios, regulatorios y contractuales, Derechos de propiedad intelectual, revisión independiente de la seguridad de la información y cumplimiento con políticas, reglas y normas de seguridad de la información y seguridad para el acceso a la información de Consultas RENIEC.* *Asimismo, coordina con la OILCC los lineamientos relacionados en materia de gestión de riesgos de seguridad de la información; tales como activos de información, clasificación de la información, entre otros que sean pertinentes, para la actualización de los documentos normativos que correspondan.*	
VII. DISPOSICIONES ESPECIFICAS	***VII. DISPOSICIONES ESPECIFICAS***	*Ninguno*
7.1 Párrafo vigente	*7.1 Párrafo vigente*	*Ninguno*
7.1.1 Párrafo vigente	*7.1.1 Párrafo vigente*	*Ninguno*
7.1.1.1 Párrafo vigente *El Titular de la entidad pública 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*	*7.1.1.1 Párrafo modificado* *La SGEN a través del OSCD propone la política de seguridad de la información y es revisada por el Comité de Gobierno y Transformación Digital quien a su vez eleva a la instancia correspondiente, para la aprobación de la JNAC mediante Resolución Jefatural.*	*Modificado*
7.1.1.2 Párrafo vigente ***La máxima autoridad administrativa o la que haga sus veces en la entidad pública 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,*	*7.1.1.2 Párrafo modificado* *La política de seguridad de la información establece el enfoque de la organización para gestionar los objetivos de seguridad de la información, publicada y difundida, para conocimiento y aplicación de los servidores civiles de la organización y acceso de las partes externas relevantes. Asimismo, la política de seguridad de la información es revisada de forma periódica (cada año) o cuando ocurran cambios*	*Modificado*

procedimientos y marco normativo en materia de seguridad y confianza digital en la entidad pública.	*significativos de la NTP o normativa legal.*	
7.1.2 Párrafo vigente	*7.1.2 Párrafo vigente*	*Ninguno*
7.1.2.1 Párrafo vigente *Los roles y responsabilidades en la organización, en cuanto a seguridad de la información, son propuestas por el OSCD, y aprobadas por la Alta Dirección, bajo una estructura organizativa de seguridad de la información la cual se encuentra detallada en el "Manual de Gestión de Seguridad de la Información".*	*7.1.2.1 Párrafo modificado* *Los roles y responsabilidades en la organización, en cuanto a seguridad de la información, son propuestas por la SGEN a través del OSCD, y aprobadas por la Alta Dirección, bajo una estructura organizativa detallada en el "Manual de Gestión de Seguridad de la Información".*	*Modificado*
7.1.3 Párrafo vigente	*7.1.3 Párrafo vigente*	*Ninguno*
7.1.3.1 Párrafo vigente *El RENIEC, cuenta con un Manual de Clasificador de Cargos del Registro Nacional de Identificación y Estado Civil – RENIEC, en el que se describen de manera ordenada todos los cargos de la entidad, estableciendo su denominación, clasificación, funciones y requisitos mínimos para el cumplimiento de objetivos de la entidad; adicionalmente se cuenta con el Reglamento de Organización y Funciones – ROF, donde se detallan las funciones y responsabilidades de los órganos y unidades orgánicas.*	*7.1.3.1 Párrafo modificado* *El RENIEC, cuenta con:* *a. El Reglamento de Organización y Funciones y Estructura Orgánica - ROF, donde se detallan las funciones, responsabilidades y niveles de la estructura de la entidad.* *b. El Manual de Clasificador de Cargos del Registro Nacional de Identificación y Estado Civil - RENIEC MCC, en el que se describen de manera ordenada todos los cargos de la entidad, estableciendo su denominación, clasificación, funciones y requisitos mínimos para el cumplimiento de objetivos de la entidad*	*Modificado*
7.1.3.2 Párrafo vigente *La segregación de funciones es un método de control basado en roles; con el fin de definir la actividad a desarrollar por cada integrante de la estructura organizativa de la institución, para el caso del SGSI, los roles y responsabilidades se encuentran detallados en el "Manual de Gestión de Seguridad de la Información". Documento que señala que los dueños de los procesos disponen de una matriz de requisitos de competencias para los roles inmersos en el Anexo "Matriz de Requisitos de Competencia para Roles", el mismo que define que el personal propuesto para labores de seguridad de la información tenga un*	*7.1.3.2 Párrafo vigente* *La segregación de funciones es un método de control basado en roles; con el fin de definir la actividad a desarrollar por cada integrante de la estructura organizativa de la institución; para el caso del SGSI los roles y responsabilidades se encuentran detallados en el "Manual de Gestión de Seguridad de la Información", documento que señala que los dueños de los procesos disponen de una matriz de requisitos de competencias , el mismo que define el perfil de formación académica y tecnológica de preferencia para el personal relacionado con las labores de seguridad de la información.*	*Ninguno*

perfil de formación académica tecnológica preferente.		
7.1.4 Párrafo vigente	*7.1.4 Párrafo vigente*	*Ninguno*
7.1.4.1 Párrafo vigente ***La JNAC demuestra su responsabilidad y compromiso con la Seguridad de la Información:*** ***a. Aprobando la política de Seguridad de la Información.*** ***b. Participando en las revisiones para la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información y en las reuniones del Comité de Gobierno y Transformación Digital.*** *c. Impulsando la aplicación de la seguridad de la información en el RENIEC, basado en la Política y Objetivos de Seguridad de la Información.*	*7.1.4.1 Párrafo modificado* *La Alta Dirección manifiesta su compromiso con la Seguridad de la Información, dando cumplimiento con las siguientes acciones:* *a. Aprobar la política de Seguridad de la Información.* *b. Impulsar la aplicación de la seguridad de la información a todos los Dueños del proceso, órganos y unidades orgánicas sobre la base de la Política y Objetivos de Seguridad de la Información del RENIEC.*	*Modificado*
7.1.5 Párrafo vigente	*7.1.5 Párrafo vigente*	*Ninguno*
7.1.5.1 Párrafo vigente *El RENIEC cuenta con un Reglamento Interno de Seguridad y de la entidad, conforme a lo dispuesto en la Ley N° 29783 – Ley de Seguridad y Salud en el Trabajo - el cual incluye las referencias en casos de emergencia, como instituciones de salud, Policía Nacional, bomberos, defensa civil, entre otros; según el ROF, la OPH tiene la responsabilidad de gestionar las acciones del Sistema de Gestión de la Seguridad y Salud en el Trabajo.*	-	*Eliminado*
	7.1.5.1 Nuevo Párrafo *La OCP supervisa y evalúa las políticas y estrategias de la gestión de comunicación institucional, comunicación digital, prensa, publicidad, protocolo, relaciones institucionales y acciones de responsabilidad social; velando por la identidad, la imagen y la reputación de la institución.* *Asimismo, evalúa la relación de la institución con los medios de comunicación, entidades públicas o privadas de carácter regional, nacional e internacional; así como*	*Incluido*

	otras asociaciones y organizaciones no gubernamentales.	
	7.1.5.2 Nuevo Párrafo *La OPH gestiona acuerdos o convenios de cooperación interinstitucional con entidades públicas o privadas, nacionales o extranjeras, en el ámbito de su competencia en beneficio de los servidores en coordinación con el órgano o unidad orgánica competente para dicho fin.*	*Incluido*
	7.1.5.3 Nuevo Párrafo *La DCSD gestiona los convenios de suministro de información con entidades privadas y públicas a ser suscritos, y los servicios disponibles de la institución.*	*Incluido*
7.1.6 Párrafo vigente	*7.1.6 Párrafo vigente*	*Ninguno*
7.1.6.1 Párrafo vigente	*7.1.6.1 Párrafo vigente*	*Ninguno*
7.1.6.2 Párrafo vigente	*7.1.6.2 Párrafo vigente*	*Ninguno*
7.1.6.3 Párrafo vigente	*7.1.6.3 Párrafo vigente*	*Ninguno*
7.1.7 Párrafo vigente	*7.1.7 Párrafo vigente*	*Ninguno*
7.1.7.1 Párrafo vigente	*7.1.7.1 Párrafo vigente*	*Ninguno*
7.1.7.2 Párrafo vigente	*7.1.7.2 Párrafo vigente*	*Ninguno*
7.1.7.3 Párrafo vigente	*7.1.7.3 Párrafo vigente*	*Ninguno*
7.1.7.4 Párrafo vigente	*7.1.7.4 Párrafo vigente*	*Ninguno*
7.1.7.5 Párrafo vigente	*7.1.7.5 Párrafo vigente*	*Ninguno*
7.1.8 Párrafo vigente	*7.1.8 Párrafo vigente*	*Ninguno*
7.1.8.1 Párrafo vigente	*7.1.8.1 Párrafo vigente*	*Ninguno*
7.1.8.2 Párrafo vigente	*7.1.8.2 Párrafo vigente*	*Ninguno*
7.1.9 Párrafo vigente	*7.1.9 Párrafo vigente*	*Ninguno*
7.1.9.1 Párrafo vigente	*7.1.9.1 Párrafo vigente*	*Ninguno*
7.1.9.2 Párrafo vigente	*7.1.9.2 Párrafo vigente*	*Ninguno*
7.1.10.1 Párrafo vigente	*7.1.10.1 Párrafo vigente*	*Ninguno*
7.1.10.2 Párrafo vigente	*7.1.10.2 Párrafo vigente*	*Ninguno*

7.1.10.3 Párrafo vigente	*7.1.10.3 Párrafo vigente*	*Ninguno*
7.1.10.4 Párrafo vigente	*7.1.10.4 Párrafo vigente*	*Ninguno*
7.1.11 Párrafo vigente	*7.1.11 Párrafo vigente*	*Ninguno*
7.1.11.1 Párrafo vigente *Mediante el documento normativo "Entrega de puesto de los servidores civiles del RENIEC", se establecen las pautas para la entrega de puesto, el cual incluye entre otros la entrega de activos de información de acuerdo con el Anexo Acta de Entrega de Puesto.*	*7.1.11.1 Párrafo modificado* *Mediante documento normativo "Entrega de puesto de los servidores civiles del RENIEC", se establecen las pautas para la entrega de puesto, el cual contempla entre otros la entrega de activos de información de acuerdo con el Anexo N° 1, Acta de Entrega de Puesto.*	*Modificado*
7.1.11.2 Párrafo vigente	*7.1.11.2 Párrafo vigente*	*Ninguno*
7.1.11.3 Párrafo vigente	*7.1.11.3 Párrafo vigente*	*Ninguno*
7.1.12 Párrafo vigente	*7.1.12 Párrafo vigente*	*Ninguno*
7.1.12.1 Párrafo vigente	*7.1.12.1 Párrafo vigente*	*Ninguno*
7.1.12.2 Párrafo vigente	*7.1.12.2 Párrafo vigente*	*Ninguno*
7.1.12.3 Párrafo vigente	*7.1.12.3 Párrafo vigente*	*Ninguno*
7.1.12.4 Párrafo vigente	*7.1.12.4 Párrafo vigente*	*Ninguno*
7.1.12.5 Párrafo vigente	*7.1.12.5 Párrafo vigente*	*Ninguno*
7.1.12.6 Párrafo vigente	*7.1.12.6 Párrafo vigente*	*Ninguno*
7.1.13 Párrafo vigente	*7.1.13 Párrafo vigente*	*Ninguno*
7.1.13.1 Párrafo vigente	*7.1.13.1 Párrafo vigente*	*Ninguno*
7.1.13.2 Párrafo vigente	*7.1.13.2 Párrafo vigente*	*Ninguno*
7.1.14. Párrafo vigente	*7.1.14. Párrafo vigente*	*Ninguno*
7.1.14.1 Párrafo vigente	*7.1.14.1 Párrafo vigente*	*Ninguno*
7.1.14.2 Párrafo vigente	*7.1.14.2 Párrafo vigente*	*Ninguno*
7.1.14.3 Párrafo vigente	*7.1.14.3 Párrafo vigente*	*Ninguno*
7.1.14.4 Párrafo vigente	*7.1.14.4 Párrafo vigente*	*Ninguno*
7.1.14.5 Párrafo vigente	*7.1.14.5 Párrafo vigente*	*Ninguno*
7.1.14.6 Párrafo vigente	*7.1.14.6 Párrafo vigente*	*Ninguno*
7.1.14.7 Párrafo vigente	*7.1.14.7 Párrafo vigente*	*Ninguno*
7.1.15 Párrafo vigente	*7.1.15 Párrafo vigente*	*Ninguno*

7.1.15.1 Párrafo vigente	*7.1.15.1 Párrafo vigente*	*Ninguno*
7.1.15.2 Párrafo vigente	*7.1.15.2 Párrafo vigente*	*Ninguno*
7.1.15.3 Párrafo vigente	*7.1.15.3 Párrafo vigente*	*Ninguno*
7.1.15.4 Párrafo vigente	*7.1.15.4 Párrafo vigente*	*Ninguno*
7.1.15.5 Párrafo vigente	*7.1.15.5 Párrafo vigente*	*Ninguno*
7.1.16 Párrafo vigente	*7.1.16 Párrafo vigente*	*Ninguno*
7.1.16.1 Párrafo vigente	*7.1.16.1 Párrafo vigente*	*Ninguno*
7.1.16.2 Párrafo vigente	*7.1.16.2 Párrafo vigente*	*Ninguno*
7.1.16.3 Párrafo vigente	*7.1.16.3 Párrafo vigente*	*Ninguno*
7.1.16.4 Párrafo vigente	*7.1.16.4 Párrafo vigente*	*Ninguno*
7.1.16.5 Párrafo vigente	*7.1.16.5 Párrafo vigente*	*Ninguno*
7.1.16.6 Párrafo vigente	*7.1.16.6 Párrafo vigente*	*Ninguno*
7.1.17 Párrafo vigente	*7.1.17 Párrafo vigente*	*Ninguno*
7.1.17.1 Párrafo vigente	*7.1.17.1 Párrafo vigente*	*Ninguno*
7.1.17.2 Párrafo vigente	*7.1.17.2 Párrafo vigente*	*Ninguno*
7.1.18 Párrafo vigente	*7.1.18 Párrafo vigente*	*Ninguno*
7.1.18.1 Párrafo vigente	*7.1.18.1 Párrafo vigente*	*Ninguno*
7.1.18.2 Párrafo vigente	*7.1.18.2 Párrafo vigente*	*Ninguno*
7.1.18.3 Párrafo vigente	*7.1.18.3 Párrafo vigente*	*Ninguno*
7.1.18.4 Párrafo vigente	*7.1.18.4 Párrafo vigente*	*Ninguno*
7.1.18.5 Párrafo vigente	*7.1.18.5 Párrafo vigente*	*Ninguno*
7.1.19 Párrafo vigente	*7.1.19 Párrafo vigente*	*Ninguno*
7.1.19.1 Párrafo vigente	*7.1.19.1 Párrafo vigente*	*Ninguno*
7.1.19.2 Párrafo vigente	*7.1.19.2 Párrafo vigente*	*Ninguno*
7.1.19.3 Párrafo vigente	*7.1.19.3 Párrafo vigente*	*Ninguno*
7.1.20 Párrafo vigente	*7.1.20 Párrafo vigente*	*Ninguno*
7.1.20.1 Párrafo vigente	*7.1.20.1 Párrafo vigente*	*Ninguno*
7.1.20.2 Párrafo vigente	*7.1.20.2 Párrafo vigente*	*Ninguno*
7.1.21 Párrafo vigente	*7.1.21 Párrafo vigente*	*Ninguno*

7.1.21.1 Párrafo vigente	*7.1.21.1 Párrafo vigente*	*Ninguno*
7.1.22 Párrafo vigente	*7.1.22 Párrafo vigente*	*Ninguno*
7.1.22.1 Párrafo vigente	*7.1.22.1 Párrafo vigente*	*Ninguno*
7.1.23 Párrafo vigente	*7.1.23 Párrafo vigente*	*Ninguno*
7.1.23.1 Párrafo vigente	*7.1.23.1 Párrafo vigente*	*Ninguno*
7.1.23.2 Párrafo vigente	*7.1.23.2 Párrafo vigente*	*Ninguno*
7.1.24 Párrafo vigente	*7.1.24 Párrafo vigente*	*Ninguno*
7.1.24.1 Párrafo vigente	*7.1.24.1 Párrafo vigente*	*Ninguno*
7.1.25 Párrafo vigente	*7.1.25 Párrafo vigente*	*Ninguno*
7.1.25.1 Párrafo vigente	*7.1.25.1 Párrafo vigente*	*Ninguno*
7.1.26 Párrafo vigente	*7.1.26 Párrafo vigente*	*Ninguno*
7.1.26.1 Párrafo vigente	*7.1.26.1 Párrafo vigente*	*Ninguno*
7.1.27 Párrafo vigente	*7.1.27 Párrafo vigente*	*Ninguno*
7.1.27.1 Párrafo vigente	*7.1.27.1 Párrafo vigente*	*Ninguno*
7.1.27.2 Párrafo vigente	*7.1.27.2 Párrafo vigente*	*Ninguno*
7.1.27.3 Párrafo vigente	*7.1.27.3 Párrafo vigente*	*Ninguno*
7.1.27.4 Párrafo vigente	*7.1.27.4 Párrafo vigente*	*Ninguno*
7.1.28 Párrafo vigente	*7.1.28 Párrafo vigente*	*Ninguno*
7.1.28.1 Párrafo vigente	*7.1.28.1 Párrafo vigente*	*Ninguno*
7.1.28.2 Párrafo vigente	*7.1.28.2 Párrafo vigente*	*Ninguno*
7.1.29 Párrafo vigente	*7.1.29 Párrafo vigente*	*Ninguno*
7.1.29.1 Párrafo vigente	*7.1.29.1 Párrafo vigente*	*Ninguno*
7.1.29.2 Párrafo vigente	*7.1.29.2 Párrafo vigente*	*Ninguno*
7.1.30 Párrafo vigente	*7.1.30 Párrafo vigente*	*Ninguno*
7.1.30.1 Párrafo vigente	*7.1.30.1 Párrafo vigente*	*Ninguno*
7.1.30.2 Párrafo vigente	*7.1.30.2 Párrafo vigente*	*Ninguno*
7.1.30.3 Párrafo vigente	*7.1.30.3 Párrafo vigente*	*Ninguno*
7.1.30.4 Párrafo vigente	*7.1.30.4 Párrafo vigente*	*Ninguno*
7.1.30.5 Párrafo vigente	*7.1.30.5 Párrafo modificado*	*Modificado*

La OTI/UIST, elabora y mantiene actualizado el inventario del software instalado en los equipos del servidor civil del RENIEC. En aquellos casos en que se detecten anomalías o licencias sin regularizar, la OTI/UIST informa al responsable del órgano o unidad orgánica involucrada y al OSCD, quienes posteriormente comunicaran a la OPH/ USTPAD a fin de que se realice las investigaciones administrativas correspondientes y el deslinde de responsabilidades.	*La OTI/UIST, elabora y mantiene actualizado el inventario del software instalado en los equipos del servidor civil del RENIEC. En aquellos casos en que se detecten anomalías o licencias sin regularizar, la OTI/UIST informa al responsable del órgano o unidad orgánica involucrada y al OSCD, quienes comunican a la OPH/ USTPAD, para las investigaciones administrativas correspondientes y el deslinde de responsabilidades.*	
7.1.30.6 Párrafo vigente	*7.1.30.6 Párrafo vigente*	*Ninguno*
7.1.31 Párrafo vigente	*7.1.31 Párrafo vigente*	*Ninguno*
7.1.31.1 Párrafo vigente	*7.1.31.1 Párrafo vigente*	*Ninguno*
7.1.31.2 Párrafo vigente	*7.1.31.2 Párrafo vigente*	*Ninguno*
7.1.31.3 Párrafo vigente	*7.1.31.3 Párrafo vigente*	*Ninguno*
7.1.32 Párrafo vigente	*7.1.32 Párrafo vigente*	*Ninguno*
7.1.32.1 Párrafo vigente	*7.1.32.1 Párrafo vigente*	*Ninguno*
7.1.32.2 Párrafo vigente	*7.1.32.2 Párrafo vigente*	*Ninguno*
7.1.33 Párrafo vigente	*7.1.33 Párrafo vigente*	*Ninguno*
7.1.33.1 Párrafo vigente	*7.1.33.1 Párrafo vigente*	*Ninguno*
7.1.33.2 Párrafo vigente	*7.1.33.2 Párrafo vigente*	*Ninguno*
7.1.34 Párrafo vigente	*7.1.34 Párrafo vigente*	*Ninguno*
7.1.34.1 Párrafo vigente	*7.1.34.1 Párrafo vigente*	*Ninguno*
7.1.34.2 Párrafo vigente	*7.1.34.2 Párrafo vigente*	*Ninguno*
7.1.35 Párrafo vigente	*7.1.35 Párrafo vigente*	*Ninguno*
7.1.35.1 Párrafo vigente	*7.1.35.1 Párrafo vigente*	*Ninguno*
7.1.35.2 Párrafo vigente	*7.1.35.2 Párrafo vigente*	*Ninguno*
7.1.35.3 Párrafo vigente	*7.1.35.3 Párrafo vigente*	*Ninguno*
7.1.35.4 Párrafo vigente	*7.1.35.4 Párrafo vigente*	*Ninguno*
7.1.35.5 Párrafo vigente	*7.1.35.5 Párrafo vigente*	*Ninguno*
7.1.35.6 Párrafo vigente *La difusión de los procedimientos se efectúa a través del Sistema Integrado de Trámite Documentario -*	*7.1.35.6 Párrafo modificado* *La difusión de los procedimientos se efectúa a través del Sistema Integrado de Trámite Documentario -*	*Modificado*

SITD, mediante Memorando Múltiple desplegado por la OPPM dirigido a los diversos órganos del RENIEC, los cuales deben comunicar a sus respectivas unidades orgánicas y estos a su vez a todo el personal bajo su cargo.	*SITD, mediante Memorando Múltiple por la OPPM dirigido a los diversos órganos del RENIEC, los cuales deben desplegar comunicación a sus respectivas unidades orgánicas y estos a su vez a todo el personal bajo su cargo.*	
7.1.36 Párrafo vigente	*7.1.36 Párrafo vigente*	*Ninguno*
7.1.36.1 Párrafo vigente *La DCSD, debe suspender el servicio del convenio con reconocimiento de costos a la empresa cuando se detecte la no actualización (bajas) de los usuarios finales, suspensión que queda sin efecto una vez subsanada dicha situación, procediendo a la reactivación del servicio.*	-	*Eliminado*
7.1.36.2 Párrafo vigente *La DCSD, debe desactivar el acceso a todos aquellos usuarios finales que no hayan realizado uso de las consultas durante un plazo máximo de 30 días, siendo el coordinador de la entidad, el responsable de realizar nuevamente la habilitación del usuario.*	-	*Eliminado*
	7.1.36.1 Nuevo Párrafo *La DCSD, debe:* *a. Suspender el servicio del convenio con reconocimiento de costos a la empresa cuando se detecte la no actualización (bajas) de los usuarios finales, suspensión que queda sin efecto una vez subsanada dicha situación, procediendo a la reactivación del servicio.* *b. Desactivar el acceso a todos aquellos usuarios finales que no hayan realizado uso de las consultas durante un plazo máximo de 30 días, siendo el coordinador de la entidad, el responsable de realizar nuevamente la habilitación del usuario.*	*Incluido*
7.1.36.2 Párrafo vigente	*7.1.36.2 Párrafo vigente*	*Ninguno*
7.1.36.3 Párrafo vigente	*7.1.36.3 Párrafo vigente*	*Ninguno*
7.1.36.4 Párrafo vigente	*7.1.36.4 Párrafo vigente*	*Ninguno*

7.1.36.5 Párrafo vigente	*7.1.36.5 Párrafo vigente*	*Ninguno*
7.1.36.6 Párrafo vigente	*7.1.36.6 Párrafo vigente*	*Ninguno*
7.1.36.7 Párrafo vigente	*7.1.36.7 Párrafo vigente*	*Ninguno*
7.1.36.8 Párrafo vigente	*7.1.36.8 Párrafo vigente*	*Ninguno*
7.1.36.9 Párrafo vigente	*7.1.36.9 Párrafo vigente*	*Ninguno*
7.1.36.10 Párrafo vigente	*7.1.36.10 Párrafo vigente*	*Ninguno*
7.1.36.11 Párrafo vigente	*7.1.36.11 Párrafo vigente*	*Ninguno*
7.1.36.12 Párrafo vigente	*7.1.36.12 Párrafo vigente*	*Ninguno*
7.1.36.13 Párrafo vigente	*7.1.36.13 Párrafo vigente*	*Ninguno*
7.1.36.14 Párrafo vigente	*7.1.36.14 Párrafo vigente*	*Ninguno*
7.1.36.15 Párrafo vigente	*7.1.36.15 Párrafo vigente*	*Ninguno*
7.1.36.16 Párrafo vigente	*7.1.36.16 Párrafo vigente*	*Ninguno*
VIII. DISPOSICIÓN COMPLEMENTARIA	***VIII. DISPOSICIÓN COMPLEMENTARIA***	*Ninguno*
8.1 Párrafo vigente	*8.1 Párrafo vigente*	*Ninguno*
8.2 Párrafo vigente	*8.2 Párrafo vigente*	*Ninguno*
8.3 Párrafo vigente	*8.3 Párrafo vigente*	*Ninguno*
IX. VIGENCIA	*IX. VIGENCIA*	*Ninguno*
X. APROBACIÓN	*X. APROBACIÓN*	*Ninguno*
XI. ANEXOS	*XI. ANEXOS*	*Ninguno*