MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

PROCESO DE CERTIFICACIÓN DIGITAL

RESOLUCION SECRETARIAL N° /30 -2018-SGEN/RENIEC		
MGSI-203-GRCD/001	VERSIÓN: 01	FECHA DE APROBACION 05 OCT. 2018
	N° PÁGINAS: 36	

INDICE

I. OBJETO Y CAMPO DE APLICACIÓN

Especificar los elementos principales del Sistema de Gestión de Seguridad de la Información del Proceso de Certificación Digital del Registro Nacional de Identificación y Estado Civil en adelante RENIEC, en el ámbito de la ECERNEP y ECEP del RENIEC, con el fin de cumplir los requisitos establecidos en la Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información - Requisitos.

II. REFERENCIAS NORMATIVAS

El Sistema de Gestión de Seguridad de la Información de la Gerencia de Registros de Certificación Digital, ha sido diseñado de acuerdo a lo establecido en:

2.1 **Constitución Política del Perú de 1993**, del 30 de diciembre de 1993.

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

2.3 **Ley N° 27269**, Ley de Firmas y Certificados Digitales, del 28 de mayo del 2000, y sus modificatorias.

2.4 **Ley N° 29733**, Ley de Protección de Datos Personales, del 03 de julio de 2011 y sus modificatorias.

2.5 **Decreto Supremo N° 015-1998-PCM**, que aprueba el Reglamento de Inscripciones del Registro Nacional de Identificación y Estado Civil, del 25 de abril de 1998.

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

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

2.8 **Decreto Supremo N° 006-2017-JUS**, que aprueba el Texto Único Ordenado de la Ley N° 27444 - Ley del Procedimiento Administrativo General, del 20 de marzo del 2017, y sus modificatorias.

2.9 **Resolución Ministerial N° 004-2016-PCM**, aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 "Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos". 2ª. Edición", en todas las entidades integrantes del Sistema Nacional de Informática, del 14 de enero de 2016, y su modificatoria.

2.10 **Resolución Ministerial N° 166-2017-PCM**, modifica el artículo 5 de la Resolución Ministerial N° 004-2016-PCM respecto al Comité de Gestión de Seguridad de la Información, define sus funciones, y establece el rol del Oficial de Seguridad de la Información, del 20 de junio de 2017.

2.11 **Resolución Jefatural N° 73-2015-JNAC/RENIEC**, que aprueba la Política de Seguridad de la Información y los Objetivos de Seguridad de la Información del RENIEC, del 30 de marzo de 2015.

2.12 **Resolución Jefatural N° 73-2016-JNAC/RENIEC**, que aprueba el Reglamento de Organización y Funciones y la Estructura Orgánica del RENIEC, del 01 de junio de 2016, y su modificatoria.

2.13 **Resolución Jefatural N° 74-2016-JNAC/RENIEC**, que aprueba el Cuadro de Codificación y Siglas de los órganos y unidades orgánicas del RENIEC, del 14 de junio de 2016.

2.14 **Resolución Secretarial N° 55-2017/SGEN/RENIEC**, que aprueba la Directiva DI-200-GPP/001 Lineamientos para la Formulación de los Documentos Normativos del RENIEC – Sexta Versión, del 28 de agosto de 2017.

2.15 **Norma Internacional ISO/IEC 27000** "Sistemas de Gestión de Seguridad de la Información – Términos, Definiciones - Vocabulario".

2.16 **Norma Internacional ISO/IEC 27001:2013** "Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos".

2.17 **Resolución Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias N° 129-2014/CNB-INDECOPI**, aprueba como Norma Técnica Peruana "NTP-ISO/IEC 27001:2014; Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos", 2ª. Edición, del 01 de diciembre de 2014.

III. DEFINICIÓN DE TÉRMINOS

3.1 El presente Manual de Seguridad de Información "Sistema de Gestión de Seguridad de la Información del Proceso de Certificación Digital", se basa en los términos y definiciones establecidos en la **Norma ISO/IEC 27000 Sistemas de Gestión de Seguridad de la Información – Términos, Definiciones – Vocabulario.**

Asimismo, se han utilizado términos y definiciones de documentos normativos del RENIEC relacionados al Sistema de Gestión de Seguridad de la Información (SGSI).

3.2 Abreviaciones

Dentro del presente manual podrán utilizarse las siguientes abreviaciones:

SIGLA	NOMBRES
AAC	Autoridad Administrativa Competente
CIGSI	Comité Interno de Gestión de Seguridad de la Información
CGSI	Comité de Gestión de Seguridad de la Información
ECEP	Entidad de Certificación para el Estado Peruano
ECERNEP	Entidad de Certificación Nacional para el Estado Peruano
ER	Escuela Registral
EREP	Entidad de Registro o Verificación para el Estado Peruano

GCI	Gerencia de Calidad e Innovación
GRCD	Gerencia de Registros de Certificación Digital
IOFE	Infraestructura Oficial de Firma Electrónica
JNAC	Jefatura Nacional
RAD	Representante de la Alta Dirección
RENIEC	Registro Nacional de Identificación y Estado Civil
ROF	Reglamento de Organización y Funciones
SGCID	Sub Gerencia de Certificación e Identidad Digital
SGREGD	Sub Gerencia de Regulación Digital
SGSI	Sistema de Gestión de Seguridad de la Información
OSDN	Oficina de Seguridad y Defensa Nacional

IV. CONTEXTO DE LA ORGANIZACIÓN

4.1 Registro Nacional de Identificación y Estado Civil (RENIEC)

El RENIEC, es un organismo público autónomo que cuenta con personería jurídica de derecho público interno, goza de atribuciones exclusivas y excluyentes en materia registral, técnica, administrativa, económica y financiera. Fue creado por Ley No 26497 del 12 de julio de 1995 con arreglo a lo previsto en los Artículos 177° y 183° de la Constitución Política del Perú. Es el organismo técnico responsable de organizar y mantener el Registro Único de Identificación de las Personas Naturales, adoptar mecanismos que garanticen la seguridad de la confección de los documentos de identidad e inscribir los hechos y actos relativos a su capacidad y estado civil, así como asegurar la confiabilidad de la información que resulta de la inscripción.

En el marco de lo dispuesto por la Ley N° 27269, modificada por la Ley N° 27310, Ley de Firmas y Certificados Digitales y su Reglamento aprobado por Decreto Supremo N° 052-2008-PCM y sus modificatorias, el RENIEC es la Entidad Certificadora Nacional para el Estado Peruano, actúa como Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), Entidad de Certificación para el Estado Peruano (ECEP) y Entidad de Registro o Verificación para el Estado Peruano (EREP).

En cumplimiento del Reglamento de la Ley de Firmas y Certificados Digitales, según lo señalado en su Art. 47 y posteriores modificatorias, el RENIEC ha logrado su acreditación ante la Autoridad Administrativa Competente (AAC) de la Infraestructura Oficial de Firma Electrónica (IOFE), conforme a los roles que le fuesen asignados:

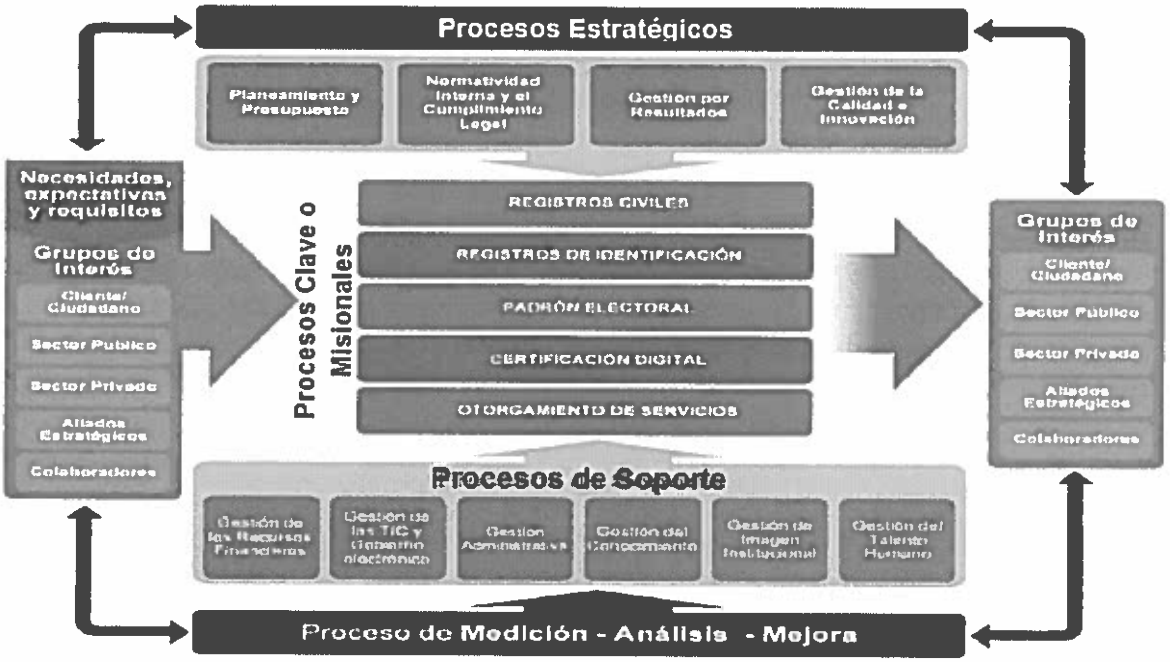
- Por Resolución N° 139-2012/CNB-INDECOPI (28DIC2012), acreditación de la ECERNEP.

- Por Resolución N° 140-2012/CNB-INDECOPI (28DIC2012), acreditación de la ECEP-RENIEC.
- Por Resolución N° 008-2013/CNB-INDECOPI (30ENE2013), acreditación de la EREP-RENIEC (Persona Natural).
- Por Resolución N° 038-2013/CNB-INDECOPI (19JUN2013), acreditación de la EREP-RENIEC (Persona Jurídica).

Con la finalidad de garantizar la seguridad y confianza, y como resultado de la mejora continua de sus procesos, el RENIEC ha logrado la certificación ISO/IEC 27001 en fecha 25SET2014 y la ISO 9001 en fecha 24SET2014 otorgadas por la Asociación Española de Normalización y Acreditación (AENOR) para las actividades del "Proceso de Certificación Digital".

El RENIEC, aplica la gestión por procesos, lo cual permite lograr un sistema de trabajo enfocado a la mejora continua del funcionamiento de las actividades de la organización mediante la identificación de procesos y la mejora de los mismos. Actualmente, el RENIEC cuenta con procesos estratégicos, procesos clave o misionales y procesos de soporte, como puede apreciarse en el siguiente gráfico:

Mapa de Procesos del RENIEC

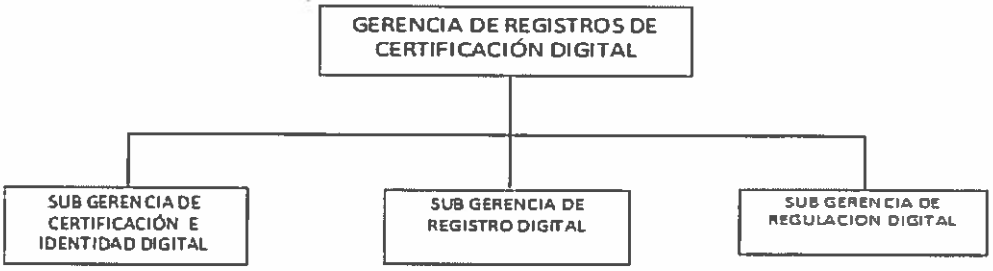


Procesos clave o misionales definidos: Registros Civiles, Registros de Identificación, Padrón Electoral, Certificación Digital y Otorgamiento de Servicios.

Mediante Resolución Jefatural N° 073-2016/JNAC/RENIEC del 01 junio de 2016 y modificatorias, se aprueba el Reglamento de Organización y Funciones y la Estructura Orgánica del RENIEC, estableciéndose disposiciones para la adecuada gestión administrativa de la institución y estableciéndose además, las funciones y facultades para cada uno de los órganos y unidades orgánicas que componen la estructura orgánica del RENIEC.

4.2 Gerencia de Registros de Certificación Digital (GRCD)

La GRCD es el órgano de línea encargado de cumplir con las funciones del RENIEC establecidas en el Reglamento de la Ley de Firmas y Certificados Digitales. Responsable de supervisar a la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), a las Entidades de Certificación para el Estado Peruano (ECEP), Entidades de Registro o Verificación para el Estado Peruano (EREP) y Prestadores de Servicios de Valor Añadido para el Estado Peruano (PSVA). Para tal efecto, la GRCD está conformada por tres unidades orgánicas, las cuales se muestran en el siguiente diagrama:



Las funciones de cada una de las Sub Gerencias se encuentran descritas en el ROF vigente, aprobado por la Jefatura Nacional del RENIEC.

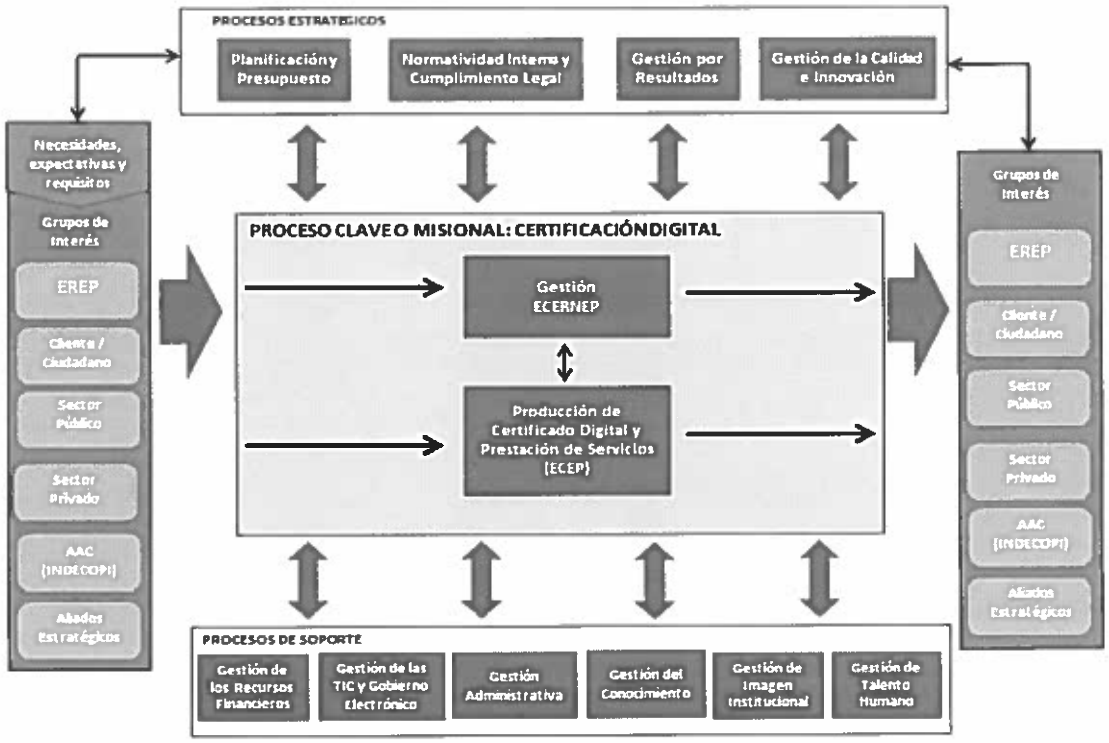
La **Sub Gerencia de Regulación Digital** (SGREGD), es la unidad orgánica encargada de representar a la Entidad de Certificación Nacional para el Estado Peruano (ECERNEP), siendo responsable de la acreditación del RENIEC como ECERNEP ante la Autoridad Administrativa Competente – AAC, y de su mantenimiento. Establece políticas y estándares para los Prestadores de Servicios de Certificación Digital de la Infraestructura Oficial de Firma Electrónica – IOFE.

La **Sub Gerencia de Certificación e Identidad Digital** (SGCID), es la unidad orgánica encargada de representar a la Entidad de Certificación para el Estado Peruano (ECEP) y al Prestador de Servicios de Valor Añadido para el Estado Peruano (PSVA), siendo responsable de la acreditación del RENIEC como ECEP y PSVA ante la Autoridad Administrativa Competente - AAC. Asimismo, es responsable de la administración de la Planta de Certificación Digital PKI.

La **Sub Gerencia de Registro Digital** (SGRD), es la unidad orgánica encargada de representar a la Entidad de Registro o Verificación para el Estado Peruano (EREP), siendo responsable de la acreditación del RENIEC como EREP ante la Autoridad Administrativa Competente - AAC. Asimismo, es responsable de la supervisión del proceso de certificación digital en las oficinas de atención del RENIEC.

La SGRD actualmente no se encuentra dentro del ámbito del alcance del Sistema de Gestión de Seguridad de Información del Proceso de Certificación Digital.

La secuencia e interacción de los procesos de realización de la SGREGD (ECERNEP) y la SGCID (ECEP) se encuentran definidas en el siguiente **Mapa de Procesos de Interacción**:



V. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

5.1 El Sistema de Gestión de Seguridad de la Información

La Gerencia de Registros de Certificación Digital ha establecido, implementado, mantiene y mejora un SGSI acorde a los requisitos de la Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información - Requisitos.

5.2 Alcance del Sistema de Gestión de Seguridad de la Información

El alcance del SGSI del proceso de Certificación Digital basado en la Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información - Requisitos, aplica a los servicios que se ejecutan en el ámbito de la ECERNEP y la ECEP, implicando la emisión y cancelación de los certificados de entidad intermedia y los certificados para entidad final desde la recepción de la solicitud de emisión del certificado digital emitido por parte de una EREP, hasta la entrega del certificado digital al solicitante, según corresponda. Siendo generado a través de los siguientes subprocesos:

- Gestión ECERNEP
- ECEP: Producción de Certificado Digital y Prestación de Servicios.

El SGSI cubrirá los sub procesos y activos de información en las siguientes ubicaciones físicas:

Proceso	Unidad Orgánica	Sede	Domicilio	Ubicación Física
Gestión ECERNEP	Sub Gerencia de Regulación Digital	Administrativa	Jr. Bolivia 109 Torre Centro Cívico Lima Centro	Piso 3
Producción de Certificado Digital y Prestación de Servicios (ECEP)	Sub Gerencia de Certificación e Identidad Digital	Administrativa	Jr. Bolivia 109 Torre Centro Cívico Lima Centro	Piso 3
		Operativa	Jr. Cusco 653 Cercado de Lima	Piso 2

5.3 Necesidades y Expectativas de las Partes Interesadas

El Plan Estratégico Institucional PEI 2012 – 2016[1] del RENIEC define como:

MISIÓN

"*Registrar la identidad, los hechos vitales y los cambios de estado civil de las personas; participar del Sistema Electoral; y promover el uso de la identificación y certificación digital, así como la inclusión social con enfoque intercultural*".

VISIÓN

"*Fortalecer la ciudadanía y el desarrollo equitativo del país como la entidad de registro del Estado Peruano que garantiza a las personas su condición de sujetos de derecho; genera confianza y seguridad jurídica; y promueve el gobierno electrónico a través de la tecnología de información y comunicaciones*".

El RENIEC, hace uso intensivo de las Tecnologías de la Información que soportan todos sus procesos, permitiendo de esta manera el logro de los objetivos estratégicos y el cumplimiento de su misión y visión, antes definidos.

De conformidad con el ROF del RENIEC, en su Artículo 10°, en los literales j), k), p) y q) se establecen las siguientes funciones relacionadas a la Seguridad de la Información:

- Velar por el irrestricto respeto del derecho a la intimidad e identidad de la persona y los demás derechos inherentes a ella derivados de su inscripción en el registro.

[1] **Resolución Jefatural N° 085-2012/JNAC/RENIEC**, aprueba el Plan Estratégico Institucional (PEI) RENIEC 2012-2016, del 21 de marzo de 2012; y su actualización mediante Resolución Jefatural N° 177-2012/JNAC/RENIEC, del 10 de julio de 2012, Resolución Jefatural N° 164-2014/JNAC/RENIEC, del 30 de junio de 2014 y Resolución Jefatural N° 166-2015/JNAC/RENIEC, del 14 de julio de 2015.

- Garantizar la privacidad de los datos relativos a las personas que son materia de inscripción.
- Mantener la confidencialidad de la información relativa a los solicitantes y titulares de certificados digitales.
- Medir y mejorar su eficacia, la calidad de su desempeño, para asegurar el cumplimiento de sus funciones, utilizando las mejores prácticas de gestión disponibles.

Encontrándose asociadas y contribuyendo estas funciones con los pilares de la Seguridad de la Información, como son: la confidencialidad, disponibilidad, e integridad de la información. En tal sentido, la Seguridad de la Información es requisito indispensable del RENIEC para cumplir con parte importante de sus funciones, para ello, debe ser apoyada por una óptima Gestión de la Seguridad de la Información a nivel institucional, implementando controles adecuados y planificados cuidadosamente.

Con la implementación del SGSI, alineado a la Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información - Requisitos, además de garantizar la confidencialidad, integridad y disponibilidad de la información y generar confianza en los ciudadanos (persona natural y jurídica), el RENIEC dará cumplimiento a lo dispuesto por la Resolución Ministerial 004-2016-PCM y Resolución Ministerial 166-2017-PCM, en relación a la implementación de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 y complementará el cumplimiento de la Ley N° 29733 y su Reglamento para la Protección de Datos Personales.

En adición a lo antes indicado, en el **Anexo N° 01 "Matriz de expectativas y necesidades de las partes interesadas respecto a la seguridad de la información"** se describen las expectativas y necesidades, que incluye las necesidades de seguridad de la información en los principales procesos del SGSI (dentro del alcance del sistema).

VI. LIDERAZGO

6.1 Liderazgo y Compromiso

La Alta Dirección evidencia su liderazgo y compromiso con el desarrollo e implementación del SGSI, a través de las siguientes actividades:

ACTIVIDADES	EVIDENCIAS
Asegurando que la política y los objetivos de la política de Seguridad de la Información se establezcan y sean compatibles con la dirección estratégica de la organización.	• Establecimiento del Plan Estratégico Institucional (PEI). • Establecimiento del Plan Operativo Institucional de la OSDN como órgano del primer nivel, que define dentro de sus objetivos, la implementación del SGSI en los procesos claves o misionales y de soporte del RENIEC.
Asegurando la integración de	• RENIEC, ha certificado y viene

los requisitos del SGSI a los procesos de la organización.	implementando el SGSI en los procesos claves o misionales de la institución, como: - Certificación Digital - Registros de Identificación - Registros Civiles - Padrón Electoral - Gestión de las TIC's y Gobierno Electrónico • La GRCD, aprueba el Plan de Tratamiento del Riesgo y Oportunidades de Seguridad de la Información. • La GRCD, emite Memorando al personal que está dentro del alcance del SGSI, indicando que todos los documentos normativos y técnicos a desarrollar deberán incluir el cumplimiento de los requerimientos de Seguridad de la Información.
Asegurando la disponibilidad de los recursos necesarios para el SGSI.	• El RENIEC a través de la Gerencia de Planificación y Presupuesto (GPP), formula su Plan Operativo y Presupuestal, dentro del cual considera la asignación de recursos para la implementación y mantenimiento de los SGSI.
Comunicando la importancia de la Gestión de la Seguridad de la Información efectiva y del cumplimiento de los requisitos del SGSI.	• El RENIEC a través de la Gerencia General (GG), emite comunicado a todas las áreas en relación a la importancia de la Gestión de la Seguridad de la Información. • Asimismo, la GRCD traslada la comunicación a todo el personal que está dentro del alcance del SGSI, solicitando el cumplimiento estricto de lo dispuesto.
Asegurando que los SGSI logren los resultados esperados.	• La OSDN, como órgano líder en la implementación del SGSI del Proceso de Certificación Digital, asesora a la GRCD, para establecer los indicadores base para la medición del cumplimiento de los objetivos de Seguridad de la Información.
Dirigiendo y apoyando a las personas para que contribuyan a la efectividad del SGSI.	• Revisiones de la Alta Dirección. • Plan de Desarrollo de Personas a cargo de la OSDN, en temas de Seguridad de la Información. • Programa de Efectividad de Controles de Seguridad de la Información. • Plan de Sensibilización.

Promoviendo la mejora continua.	• La implementación del SGSI del proceso de Certificación Digital, implica una gestión de mejora continua, basada en el modelo de gestión de procesos de Deming: Planificar-Hacer-Verificar-Actuar (PHVA).
Apoyando los roles de Gestión relevantes para demostrar su liderazgo según corresponda a sus áreas de responsabilidad.	• El RENIEC, conforme al ROF asigna a la OSDN, a través de la Sub Gerencia de Seguridad de la Información, la función de conducir la implementación del SGSI en la institución. • La GRCD comunica a la OSDN mediante memorando, la asignación de gestores líderes y operativos de Seguridad de la Información.

6.2 Política

La Alta Dirección ha definido y aprobado la Política de Seguridad de la Información del RENIEC mediante Resolución Jefatural N° 073-2015-JNAC-RENIEC, que define:

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Registro Nacional de Identificación y Estado Civil, tiene como activo principal la información de todos los peruanos registrados e identificados; preserva su confidencialidad, integridad y disponibilidad en cada uno de los procesos a través de incorporación de controles, procedimientos y metodologías definidas, personal capacitado, tecnología adecuada y mecanismos de mejora continua en el cumplimiento del marco legal vigente y estándares internacionales.

La Alta Dirección ejerce las acciones necesarias para asegurar que la Política de Seguridad de la información:

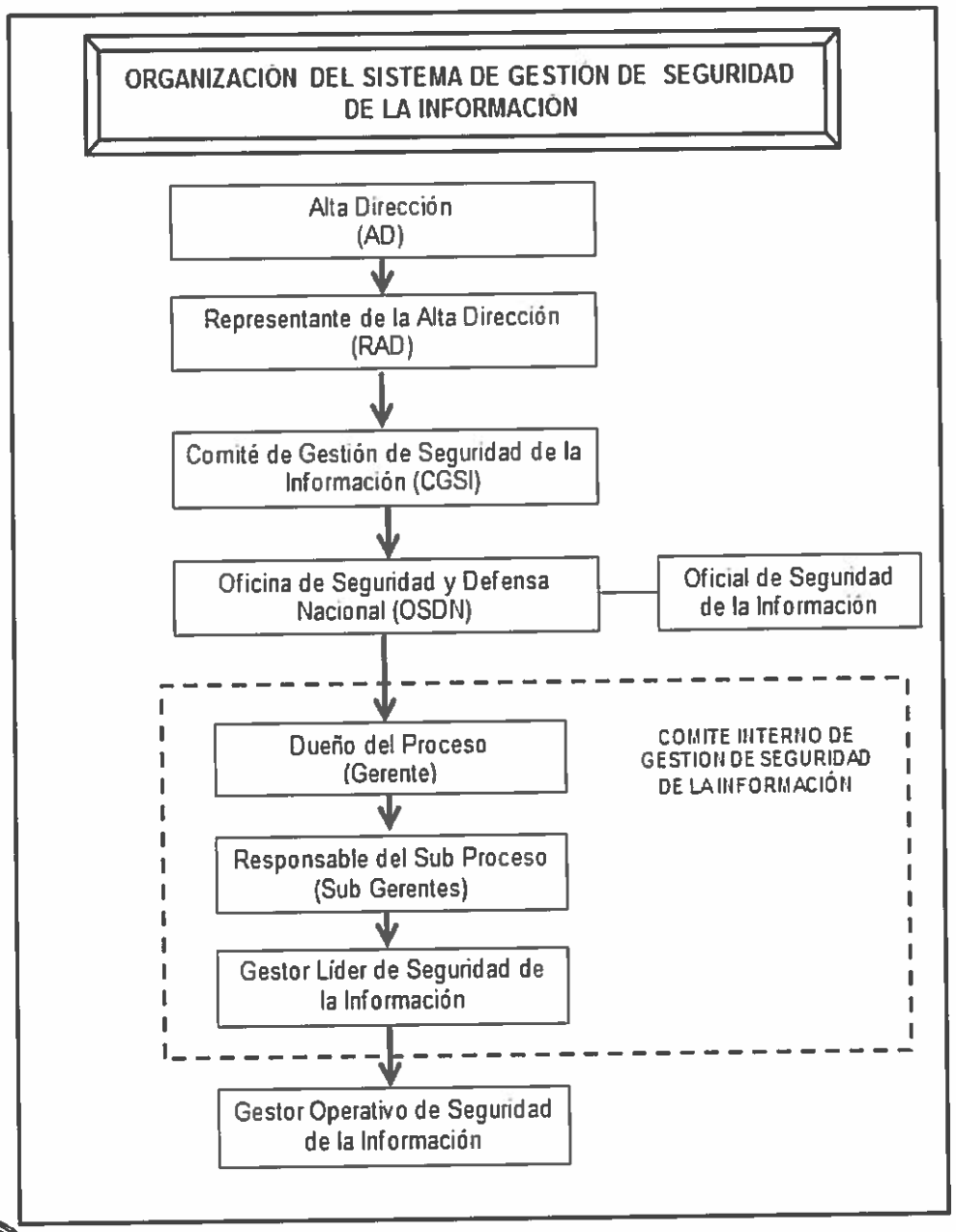
a. Se adecue a las necesidades de la entidad y de los ciudadanos.
b. Incluya el compromiso para satisfacer los requisitos y la mejora continua.
c. Proporcione un marco de referencia para establecer y revisar los objetivos de Seguridad de la Información.
d. Sea comunicada, entendida e interiorizada por todo el personal a través de:
    - Publicación en la página web del RENIEC.
    - Publicación en periódico mural y/o lugares visibles.
    - Presentación en reuniones de los trabajadores.
    - Charlas de sensibilización a los trabajadores.

- Revisión de su cumplimiento durante las auditorías internas del SGSI.
- Sistema Integrado de Trámite Documentario.

e. Sea analizada durante la Revisión por la Alta Dirección, para su continua adecuación y eficacia.

6.3 Roles, Responsabilidades y Autoridades Organizacionales

Los roles, responsabilidades y autoridades para los diferentes Órganos y Unidades Orgánicas del SGSI del proceso de Certificación Digital, están definidos en cada numeral del presente manual. Para la implementación, mantenimiento y mejora del SGSI se tiene la siguiente estructura:



6.3.1 Comité de Gestión de Seguridad de la Información (CGSI)

Es la instancia permanente de carácter no técnico y de máximo nivel sobre la Seguridad de la Información, encargado de impulsar la implementación, operación, monitoreo, revisión, mantenimiento y mejora continua del SGSI, en el RENIEC.

Está constituido mediante Resolución Jefatural N° 069-2017/JNAC/RENIEC que aprueba la conformación del Comité de Gestión de Seguridad de la Información del Registro de Identificación y Estado Civil, el mismo que está integrado por los siguientes miembros:

Representante Titular según RJ N° 069-2017-JNAC/RENIEC	Representante Suplente según RJ N° 069-2017-JNAC/RENIEC
El Jefe Nacional, quién lo presidirá	Gerente General, quien reemplazará al Presidente
Jefe de la Oficina de Seguridad y Defensa Nacional como Secretario Técnico	Sub Gerente Seguridad de la Información de la Oficina de Seguridad y Defensa Nacional, quien reemplazará al Secretario Técnico
Gerente de Administración	Sub Gerente de Servicios Generales de la Gerencia de Administración
Gerente de Planificación y Presupuesto	Sub Gerente de Racionalización y Modernización de la Gerencia de Planificación y Presupuesto
Gerente de Tecnología de la Información	Sub Gerente de Soporte Técnico Operativo de la Gerencia de Tecnología de la Información
Gerente de Asesoría Jurídica	Sub Gerente de Sistematización Jurídica de la Gerencia de Asesoría Jurídica
Oficial de Seguridad de la Información	---------
Un representante del Gabinete de Asesores de la Jefatura Nacional	Un representante del Gabinete de Asesores de la Jefatura Nacional

Las funciones del CGSI establecidas mediante Resolución Jefatural N° 032-2018/JNAC/RENIEC son las siguientes:

a. Proponer la política y objetivos de seguridad de la información alineados con el Plan Estratégico Institucional, con la Política Nacional de Gobierno Electrónico y regulación en el ámbito de seguridad de la información;

b. Promover y gestionar la implementación del Sistema de Gestión de Seguridad de la Información;

c. Promover la gestión de seguridad de la información en los procesos y cultura organizacional;

d. Gestionar la asignación del personal y recursos necesarios para la implementación del Sistema de Gestión de Seguridad de la Información;

e. Difundir la importancia de una efectiva gestión de seguridad de la información a las partes interesadas, en conformidad con los requisitos del Sistema de Gestión de Seguridad de la Información;

f. Evaluar el desempeño del Sistema de Gestión de Seguridad de la Información;

g. Otras funciones que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia.

6.3.2 Oficina de Seguridad y Defensa Nacional (OSDN)

La OSDN es el Órgano de asesoramiento de la Alta Dirección, encargado del planeamiento, programación, ejecución y supervisión de las acciones de gestión del riesgo de desastres, seguridad y defensa nacional, gestión de seguridad de la Información a nivel institucional en concordancia con las disposiciones normativas correspondientes. Responsable de la gestión del sistema de seguridad institucional que garantice la protección de las personas, de los bienes, activos de información, las instalaciones y el normal funcionamiento de los servicios del RENIEC (funciones establecidas en el ROF).

6.3.3 Oficial de Seguridad de la Información

El RENIEC a través de la Oficina de Seguridad y Defensa Nacional designará un Oficial de Seguridad de la Información, quién será responsable de coordinar la implementación del Sistema de Gestión de Seguridad de la Información en la entidad.

6.3.4 Comité Interno de Gestión de Seguridad de la Información (CIGSI)

Es la instancia permanente a nivel interno, de carácter no técnico sobre la Seguridad de la Información en el área que implementa el SGSI; encargado de gestionar las actividades relevantes para la implementación, mantenimiento y mejora continua del SGSI. Está integrado por los siguientes miembros:

Presidente	Gerente de Registros de Certificación Digital (Dueño del Proceso)
Secretario Técnico	Gestor Líder de Seguridad de la Información de la GRCD.
Miembro	Sub Gerente de Certificación e Identidad Digital
Miembro	Sub Gerente de Regulación Digital

El CIGSI se encargará de las siguientes funciones:

- Asegurar que el SGSI se ejecute conforme a los requisitos de la normatividad vigente.
- Integrar los requisitos del SGSI en las tareas que se desarrollan en la Planta de Certificación Digital PKI.
- Revisar y aprobar la documentación que sea requisito normativo del SGSI.
- Aprobar los resultados del proceso de análisis y evaluación de riesgos de Seguridad de la Información.
- Establecer los objetivos específicos de Seguridad de la Información del área y la planificación para lograrlos, concordantes con los objetivos institucionales del RENIEC.
- Gestionar la disponibilidad de recursos suficientes para desarrollar, implementar, operar, monitorear, revisar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información.
- Aprobar las competencias de Seguridad de la Información en el marco de los roles requeridos para la implementación del SGSI.
- Comunicar a todo el personal del área, la importancia de cumplir los objetivos y políticas de Seguridad de la Información, sus responsabilidades y la necesidad de la mejora continua.
- Establecer los indicadores para la medición de la efectividad del SGSI.
- Revisar y evaluar los resultados del SGSI, como mínimo una vez al año, para asegurar su conveniencia, adecuación y eficacia continua.
- Tomar las decisiones que permitan mejorar de manera continua la conveniencia, suficiencia y efectividad del SGSI.
- Otras funciones que se le asigne en el ámbito de su competencia.

6.3.5 Dueño del Proceso

Es la persona que tiene la responsabilidad y confianza para el éxito del diseño, desarrollo, ejecución y desempeño de un proceso completo.

6.3.6 Responsable del Sub proceso

Es la persona a quien el Dueño del Proceso encarga la conducción de una parte del proceso, es decir, un sub proceso.

6.3.7 Gestor Líder en Seguridad de la Información

La GRCD (Dueño del Proceso) asignará al Gestor Líder el rol, la responsabilidad y la autoridad para cumplir con las siguientes funciones:

- Velar por el cumplimiento de la política de Seguridad de la Información, documentos, directivas y normas relacionadas.

- Liderar el Equipo de Riesgos de Seguridad de la Información y la elaboración de la Declaración de Aplicabilidad.
- Elaborar la Declaración de Aplicabilidad en concordancia con el Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información.
- Monitorear la ejecución del Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información.
- Supervisar la ejecución de las actividades de sensibilización en Seguridad de la Información.
- Planificar y monitorear la evaluación de desempeño del Sistema de Gestión de Seguridad de la Información a través de los indicadores de gestión, la cual será reportada a la OSDN.
- Coordinar la elaboración y actualización del Plan de Contingencias.
- Gestionar la programación de las auditorías internas/externas del SGSI.
- Monitorear el cierre de las no conformidades y las acciones correctivas, asimismo reportará a la OSDN y CIGSI el estado de las acciones correctivas.
- Gestionar las acciones para la clasificación de la información, etiquetado y uso adecuado de los activos de Seguridad de la Información.
- Gestionar las acciones para la atención de vulnerabilidades, eventos e incidentes de Seguridad de la Información.
- Informar al CIGSI y a la OSDN, sobre el desempeño y oportunidades de mejora del SGSI.
- Otras funciones que se le asigne en el ámbito de su competencia.

Esta asignación es hecha de conocimiento de la OSDN.

6.3.8 Gestor Operativo en Seguridad de la Información

Los dueños de los subprocesos (Sub Gerentes SGCID y SGREGD), designarán al o los Gestores Operativos, los roles, las responsabilidades y la autoridad para cumplir con las siguientes funciones:

- Integrar el equipo de riesgos de Seguridad de la Información y ejecutar las actividades que demande la Gestión de Riesgos de Seguridad de la Información.
- Participar en la elaboración de la Declaración de Aplicabilidad en concordancia con el Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información.
- Ejecutar las actividades de sensibilización en Seguridad de la Información.
- Conservar la información documentada necesaria para el SGSI.
- Participar en la elaboración, actualización y prueba del Plan de Contingencias.

- Gestionar las acciones que demanden el Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información.
- Realizar la evaluación de desempeño del SGSI a través de los indicadores de gestión.
- Coordinar y participar en el desarrollo de las auditorías internas/externas, brindando la información que corresponda para la ejecución con éxito.
- Ejecutar y/o gestionar las actividades que demanden el cierre de las no conformidades y las acciones correctivas.
- Velar por que los activos de información estén debidamente inventariados y etiquetados según su clasificación, y sean utilizados de acuerdo a los procedimientos establecidos que garantizan su uso aceptable.
- Reportar y gestionar la ejecución de las acciones correctivas de las vulnerabilidades, eventos e incidentes de Seguridad de la Información.
- Comunicar los temas de su gestión al Gestor Líder de Seguridad de la Información.
- Proponer y coordinar la ejecución de controles relacionados a la Seguridad de la Información en el ámbito de su competencia.
- Otras funciones que se le asigne en el ámbito de su competencia.

Esta asignación es hecha de conocimiento de la OSDN a través de la GRCD.

6.3.9 Equipo de Riesgos

Es un grupo multifuncional conformado por el Gestor(es) Líder(es) y Operativo(s) de Seguridad de la Información. El cual es designado por los dueños del proceso y sub procesos. Sus funciones son:

- Elaborar el inventario de activos de información.
- Desarrollar la evaluación de Riesgos y Oportunidades de Seguridad de la Información, elaborar el Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información, y la evaluación del Riesgo Residual.
- Elaborar y remitir al CIGSI y la OSDN, el informe de la identificación, análisis, evaluación y tratamiento de los riesgos y oportunidades del SGSI.

VII. PLANIFICACIÓN

7.1 Acciones para Tratar los Riesgos y las Oportunidades

El RENIEC a través de la **DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información" e IN-208-OSDN/001 "Gestión de Riesgos de Seguridad de la Información"**, establece lineamientos para identificar, analizar, evaluar, y tratar los riesgos de Seguridad de la Información a los

que se encuentra expuesto, hasta obtener un nivel aceptable del riesgo y garantizar la Seguridad de la Información en las áreas que cuenten o implementen un SGSI.

7.1.1 Generalidades

La GRCD (Dueño del Proceso), debe:

a. Asegurar los resultados esperados a través de los lineamientos y las especificaciones descritas en el presente manual.

b. Desarrollar acciones para la prevención o reducción de efectos indeseados, en coordinación con los dueños de los sub procesos (SGCID y SGREGD), a fin de cumplir los objetivos y requisitos del SGSI.

c. Promover la mejora continua.

d. Identificar los riesgos y oportunidades de mejora para su tratamiento y seguimiento, aplicando la **DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información" e IN-208-OSDN/001 "Gestión de Riesgos de Seguridad de la Información".**

e. Aplicar las estrategias, controles y evaluación del riesgo residual esperado, descritos en la **DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información" e IN-208-OSDN/001 "Gestión de Riesgos de Seguridad de la Información".**

7.1.2 Valoración del Riesgo de Seguridad de la Información

7.1.2.1 Las actividades de análisis, evaluación y tratamiento de riesgos de seguridad de la información se encuentran definidas en la **DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información" e IN-208-OSDN/001 "Gestión de Riesgos de Seguridad de la Información"**, que establecen los criterios contra los cuales se evalúan los riesgos de Seguridad de la Información, los lineamientos para identificar, analizar, evaluar, y tratar los riesgos de Seguridad de la Información a los que se encuentra expuesto el proceso de Certificación Digital, hasta obtener un nivel aceptable del riesgo y garantizar la Seguridad de la Información en las áreas que cuenten o implementen un SGSI.

7.1.2.2 La GRCD, con el apoyo de la OSDN a través de los gestores operativos y gestores líderes de Seguridad de la Información, identifican las amenazas, vulnerabilidades y riesgos; posteriormente genera un Plan de Tratamiento de Riesgos bajo los criterios de disponibilidad, confidencialidad e integridad de la información. Se mantiene información documentada de este proceso.

7.1.3 Tratamiento del Riesgo de Seguridad de la Información

7.1.3.1 Los lineamientos para identificar, analizar, evaluar y tratar los riesgos del SGSI se encuentran definidos en la **DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información" e IN-208-OSDN/001 "Gestión de Riesgos de Seguridad de la Información"**, para lo cual la GRCD, SGREGD y la SGCID, establecen estrategias, responsables y tiempo estimado, para el tratamiento del riesgo, seleccionando los controles que sean necesarios hasta obtener un nivel aceptable del riesgo.

7.1.3.2 La GRCD, SGREGD y la SGCID, gestionan la implementación de los controles definidos en el Plan de Tratamiento de Riesgos e informan a la OSDN, cualquier cambio en el proceso, para realizar una re-evaluación del riesgo de Seguridad de la Información.

7.1.3.3 Se han establecido controles necesarios para el SGSI, los mismos que se encuentran expresados en la Declaración de Aplicabilidad, que incluye la justificación de las inclusiones, ya sea que se implementen o no, así como la justificación de excluir controles del Anexo A de la Norma ISO/IEC 27001:2013 "Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de Seguridad de la Información – Requerimientos".

7.1.4 Gestión de Incidentes de Seguridad de la Información

El RENIEC a través de la **DI-374-OSDN/008 "Gestión de incidentes de Seguridad de la Información"**, asegura que los eventos e incidentes de seguridad que se presenten con los activos de información, sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, y tomar oportunamente las acciones correctivas.

7.2 Objetivos de Seguridad de la Información y Planificación para conseguirlos

La Alta Dirección ha definido y aprobado los Objetivos Generales de Seguridad de la Información del RENIEC mediante Resolución Jefatural N° 073-2015/JNAC-RENIEC, y son:

OBJETIVOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

- *Proteger la confidencialidad de la información asegurando que sea accesible a organismos o personas autorizadas.*
- *Salvaguardar la integridad de la información para garantizar su exactitud y totalidad, así como sus métodos de procesamiento.*
- *Mantener la disponibilidad de la información y los sistemas de información que soportan los procesos de RENIEC para garantizar que los organismos o personas autorizadas tengan acceso a la información cuando lo requieran.*
- *Establecer, implementar, operar, monitorear, revisar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información del RENIEC.*

La GRCD ha definido y aprobado los Objetivos Específicos de Seguridad de la Información que apoyan al cumplimiento de los Objetivos Generales de Seguridad de la Información, y son:

OBJETIVOS ESPECIFICOS DE SEGURIDAD DE LA INFORMACIÓN

- *Minimizar la existencia de eventos y/o incidentes de seguridad de la información.*
- *Disminuir la pérdida de la confidencialidad, integridad y disponibilidad de la información.*
- *Incrementar el conocimiento del personal en temas de seguridad de la información.*
- *Asegurar que el sistema cumple con los requisitos de la norma vigente.*

La GRCD, comunica mediante memorando a los involucrados en el SGSI, los objetivos específicos de Seguridad de la Información para su estricto cumplimiento, y los indicadores para su medición. Así también planifica las actividades a realizar para lograr los objetivos específicos de Seguridad de la Información, mediante el formato del **Anexo N° 03 "Matriz de Planificación y Seguimiento de Objetivos de Seguridad de la Información".**

VIII. SOPORTE / APOYO

8.1 Recursos

La GRCD, la SGREGD y la SGCID, elaboran anualmente el respectivo **Plan Operativo Institucional (POI) y Cuadro de Necesidades** en base al presupuesto asignado dentro del cual incluyen las necesidades de recursos humanos, infraestructura, equipos, sistemas y otros que apoyen a la implementación y mantenimiento del SGSI del Proceso de Certificación Digital.

8.2 Competencias

8.2.1 La GRCD en coordinación con la SGCID y SGREGD, determinan las

necesidades de competencia del personal que realiza actividades que afectan la conformidad de los requisitos del SGSI, a través del presente Manual de Seguridad de la Información, y la **GP-414-ER/SGFC/001 "Formación y Capacitación de la Escuela Registral"**.

8.2.2 Los requisitos mínimos de competencia para desarrollar actividades específicas del SGSI del proceso de Certificación Digital, son definidos por los funcionarios responsables de la GRCD a través de sus analistas de personal, mediante el formato del **Anexo N° 02 "Matriz de Requisitos de Competencia para los Roles del SGSI"**.

8.2.3 La Gerencia de Talento Humano (GTH), es responsable de:

a. El proceso de selección y contratación de personal. La GRCD a través de su Analista de Personal, informa a la Gerencia de Talento Humano, la necesidad de incorporar nuevo personal, traslado o rotación de personal, detallando el rol en el SGSI y competencias, a fin de solicitar el cumplimiento de los requisitos especificados en el **Anexo N° 02 "Matriz de Requisitos de Competencia para los Roles del SGSI"**.

b. De organizar, registrar, custodiar, actualizar, depurar, mantener controlar y conservar los legajos de los servidores civiles de la entidad, conforme se encuentra establecido en la DI-406-GTH/007 "Administración del Legajo del Servidor Civil en el RENIEC". Todo personal del SGSI es responsable de remitir su documentación personal que asegure la actualización de sus legajos personales.

8.3 Concientización

8.3.1 La OSDN en atención a las necesidades de formación y sensibilización en Seguridad de la Información del personal de la GRCD, coordina con la Escuela Registral (ER) su programación y realización, definiéndose en el Plan de Desarrollo de Personas en Seguridad de la Información.

8.3.2 La Escuela Registral a través de la Sub Gerencia de Formación y Capacitación establece los procedimientos que deben observarse respecto a las actividades de coordinación previas, durante y después de la ejecución de los cursos de capacitación. Para los fines del caso, se dispone del siguiente documento normativo **NAI-457-ER/SGFC/001 "Coordinación para la Ejecución de Formación y Capacitación"**.

8.3.3 La OSDN en coordinación con los Órganos del RENIEC que cuentan con un SGSI, desarrollan un plan anual de oportunidades de mejora con la finalidad de optimizar la cultura organizacional de seguridad y el desempeño de los SGSI del RENIEC.

8.3.4 Además, a nivel interno, la GRCD a través del Gestor Líder y los Gestores Operativos, realiza actividades de concientización o

sensibilización en materia de Seguridad de la Información.

8.4 Comunicación

8.4.1 El RENIEC a través de la **DI-219-SGEN/003 "Documentos Escritos"**, establece lineamientos de cumplimiento obligatorio, que rigen la elaboración, emisión, derivación, atención y archivo de los documentos escritos impresos en papel y convertidos a documentos electrónicos, tanto para las comunicaciones internas y externas, documentos normalizados y que cuenten con el respaldo de su emisión, trámite y archivo en el Sistema Integrado de Trámite Documentario Institucional.

8.4.2 La comunicación interna entre los diferentes niveles y funciones respecto del SGSI del Proceso de Certificación Digital se realiza mediante correo electrónico, intranet, Sistema Integrado de Trámite Documentario (siguiendo lo establecido en la **DI-219-SGEN/003 "Documentos Escritos"**) y a través de reuniones de trabajo cuyos acuerdos son consolidados en actas de reunión, mesas de trabajo o lineamientos de trabajo, incidiendo principalmente en los siguientes temas:

- Cumplimiento de la Política y Objetivos de Seguridad de la Información.
- Resultados de la Gestión de Riesgos de Seguridad de la Información, auditorías y acciones correctivas.
- Resultados de la revisión del SGSI por la Alta Dirección.
- Cambios y mejoras en el SGSI.
- Y otros que sean relevantes para la seguridad de la información.

8.4.3 Cuando se planifiquen cambios en las condiciones de operación del SGSI del proceso de Certificación Digital, los responsables de los cambios deben asegurar que se hayan tomado las previsiones del caso antes de implementar dichos cambios, pudiendo realizar consultas y/o coordinaciones con las partes interesadas mediante las disposiciones antes indicadas.

8.5 Información Documentada

8.5.1 Generalidades

El SGSI del proceso de Certificación Digital, incluye:

a. La información documentada requerida por la Norma Técnica Peruana ISO/IEC 27001:2014, y
b. La información documentada establecida como necesaria para la efectividad del mismo.

8.5.2 Creación, Actualización y Control de la Información Documentada

El RENIEC a través de la **DI-200-GPP/001 "Lineamientos para la Formulación de los Documentos Normativos del RENIEC"**,

establece lineamientos para la formulación de los documentos normativos de las áreas internas; este documento normativo es administrado por la Gerencia de Planificación y Presupuesto (GPP) a través de la Sub Gerencia de Racionalización y Modernización (SGRM), y es de aplicación obligatoria para todas las áreas del RENIEC.

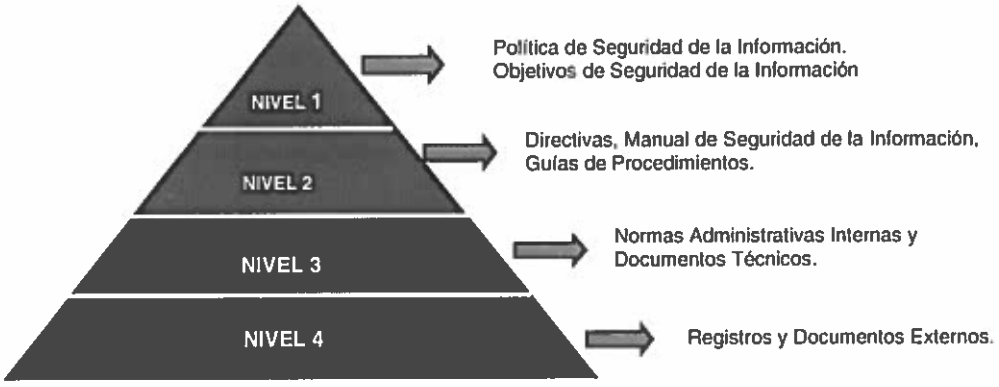
Para la formulación de documentos de carácter técnico que se aplican en el ámbito de la Planta de Certificación Digital PKI, la GRCD ha emitido el Memorando Múltiple N° 000010-2017/GRCD/RENIEC, que dispone los lineamientos para la formulación y gestión de estos documentos.

Asimismo, la GRCD, en coordinación con la OSDN, hará la difusión, almacenamiento, conservación, actualización, retención y disposición de la información documentada relacionada al cumplimiento del SGSI, cuando sea necesario y según corresponda.

8.5.3 Estructura de la Documentación

8.5.3.1 Documentos Normativos que Apoyan al SGSI

Los documentos normativos que apoyan al SGSI del proceso de Certificación Digital, garantizan que éste cuente con los documentos estrictamente necesarios y maneje la dinámica del mejoramiento continuo. En la medida que se evidencie la eficacia de las acciones tomadas y la madurez del sistema de gestión, los procesos y documentos se ajustarán y evolucionarán, a fin de cumplir con las necesidades de Seguridad de la Información; jerarquizados y clasificados de la siguiente manera:



8.5.3.2 Manual del SGSI

El CIGSI es el responsable de elaborar, controlar y actualizar el Manual de Seguridad de la Información, para dar respuesta a los requisitos de la Norma Técnica

Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información - Requisitos.

8.5.3.3 Disponibilidad de la Información

Para asegurar que los documentos normativos vigentes aplicables estén disponibles para todo el personal, se cuenta con los siguientes medios:

- Link (documentos normativos) en la intranet RENIEC
- Repositorio Digital de la Planta PKI.
- Copia física controlada (en caso se requiera).

Para el personal que no cuente con equipos informáticos se identificará un punto de uso, para ello o cuando se requiera, el funcionario responsable del proceso a través del Gestor Operativo dispondrá de copias físicas controladas debidamente identificadas con el sello **"Copia Controlada"**, registrando su distribución en el **Anexo N° 04 "Lista de Distribución de Documentos".** Cualquier copia impresa que no cuente con el sello de "Copia Controlada" y que no se encuentre registrada en la lista de distribución de documentos, será considerada como copia no controlada.

Cuando se actualiza un documento normativo, las copias controladas de la versión anterior serán recuperadas por el Gestor Operativo, para su eliminación, cuya ejecución se registrará en el **Anexo N° 05 "Acta de Eliminación".**

La Gerencia de Asesoría Jurídica (GAJ) a través de la Sub Gerencia de Sistematización Jurídica (SGSJ), establece los lineamientos y acciones a seguir para una adecuada sistematización y control de los documentos de origen externo, que afecten al SGSI, contemplada en la Guía de Procedimientos **GP-399-GAJ/SGSJ/004 "Sistematización de Documentación y Normatividad Interna y Externa del RENIEC".**

Los documentos normativos del SGSI son registrados por el Gestor Operativo, en el **"Inventario de Documentos",** que se detalla en el **Anexo N° 06.**

8.5.3.4 Clasificación de la Información

El RENIEC a través de la **DI-373-OSDN/007 "Clasificación de la Información del Sistema de Gestión de Seguridad de la Información"**, establece lineamientos a seguir para la clasificación y tratamiento de la información con independencia del medio de soporte en el que se encuentre.

8.5.3.5 Registros que Apoyan al SGSI

La GRCD, mantiene sus registros conforme a la **DI-349-GCI/004 "Control de Registros"** del RENIEC, en la que se establece lineamientos para identificar, almacenar, proteger, recuperar, retener y disponer de los registros. Siendo el Gestor Operativo, el responsable de los registros propios del SGSI.

IX. OPERACIONES

9.1 Planificación y Control Operacional

El SGSI del Proceso de Certificación Digital, planifica, implementa y controla los procesos necesarios para cumplir con los requisitos de Seguridad de la Información detallados en el numeral 7.1 y 7.2 del presente manual.

9.2 Evaluación del Riesgo de Seguridad de la Información

El SGSI del Proceso de Certificación Digital, realiza evaluaciones de riesgos de Seguridad de la Información a intervalos planificados, según lo dispuesto por la OSDN mediante memorando en el que indica que la periodicidad de la actualización de los documentos del análisis, evaluación y tratamiento de riesgos de Seguridad de la Información, será de un año, contando a partir de la aprobación del Plan de Tratamiento de Riesgos de Seguridad de la Información o cuando se produzcan cambios significativos en la Seguridad de la Información.

9.3 Tratamiento del Riesgo de Seguridad de la Información

El SGSI del proceso de Certificación Digital, planifica las actividades, responsables, fechas, etc. para tratar los riesgos de nivel importante y crítico, y realiza seguimiento mediante el Plan de Tratamiento de Riesgos de Seguridad de la Información.

X. EVALUACIÓN DEL DESEMPEÑO

10.1 Monitoreo, Medición, Análisis y Evaluación

Con el fin de demostrar la conformidad con los requisitos de la normatividad vigente y mejorar continuamente la eficacia del SGSI, la GRCD, en coordinación con la OSDN, establece indicadores relacionados a los procedimientos y controles clave que apoyan al cumplimiento de los objetivos específicos de Seguridad de la Información. Para ello se llevan a cabo actividades para el seguimiento y medición de los indicadores; de manera que se evidencie la capacidad de los procesos y controles para alcanzar los resultados planificados en cuanto a la efectividad y eficacia del SGSI. Para el uso de los indicadores del SGSI se hace uso de la **"Ficha del Indicador"** ver **Anexo N° 07.**

El resultado de las mediciones, es analizado y evaluado por el Gestor Líder de Seguridad de la Información, quien informa al Comité Interno de Seguridad de la Información y a la OSDN, a fin de proponer mejoras, o gestionar las acciones correctivas cuando no se alcancen los resultados planeados o exista riesgo de incumplimiento.

Se evalúa también la efectividad de los controles de Seguridad de la Información implementados en el SGSI, para lo cual se aplica lo dispuesto en la **DI-419-OSDN/011 "Lineamientos para la Gestión de la Efectividad de Controles de Seguridad de la Información"**.

10.2 Auditoría Interna

La GRCD, en coordinación con la GCI, planifica el desarrollo de las Auditorías Internas de los Sistemas de Gestión implementados, según los Lineamientos establecidos en la **DI-400-GCI/011 "Auditorías Internas de los Sistemas de Gestión del RENIEC"**, en la que se definen:

- Las responsabilidades y los requisitos para planificar y realizar las auditorías, incluido los criterios para la calificación de auditores; y
- Los lineamientos para informar sobre los resultados y mantener los registros asociados.

Durante la revisión por la Alta Dirección se analizan los resultados de las auditorías internas, con el objetivo de verificar la conformidad con las políticas de Seguridad de la Información, evaluando el nivel de implementación y de la capacidad de mejora del SGSI.

10.3 Revisión por la Alta Dirección

La Alta Dirección a través del RAD del RENIEC, realiza revisiones de gestión de seguridad de la información de los procesos clave o misionales de la Institución, para asegurar su conveniencia, adecuación y efectividad continua. Asimismo, comunica a la GRCD los criterios para la revisión anual de la dirección del SGSI.

La revisión debe incluir consideraciones como:

a. El estado de las acciones con relación a las revisiones anteriores por parte de la gerencia;
b. Cambios en asuntos externos e internos que son relevantes al Sistema de Gestión de Seguridad de la Información;
c. Retroalimentación sobre el desempeño de Seguridad de la Información, incluyendo tendencias en:
   - No conformidades y acciones correctivas;
   - Resultados del monitoreo y medición;
   - Resultados de auditoria; y
   - Cumplimiento de los objetivos de Seguridad de la Información;
d. Retroalimentación de partes interesadas;
e. Resultados de la evaluación de riesgo y estado del Plan de Tratamiento de Riesgos; y
f. Oportunidades para la mejora continua.

Los resultados de la Revisión por la Alta Dirección incluyen las decisiones relacionadas a las oportunidades de mejora y a cualquier necesidad de cambio, los mismos que son documentados mediante actas de la revisión de gestión, las cuales serán custodiadas por el RAD. El SGSI del Proceso de

Certificación Digital mantiene información documentada de los resultados de las revisiones de la Alta Dirección.

El Comité Interno de Seguridad de la Información, realiza reuniones periódicas en donde se revisa la marcha de la implementación y el mantenimiento del SGSI.

Y el Gestor Líder realiza el seguimiento de los acuerdos y de las acciones aprobadas y comunica el estado de los mismos al CIGSI y a la OSDN.

XI. MEJORAS

11.1 No Conformidades y Acciones Correctivas

La GRCD, gestiona las No Conformidades conforme a la **DI-421-GCI/012 "Tratamiento de Hallazgos"**, en la que se establece lineamientos para identificar, investigar y eliminar las causas de no conformidades que puedan generarse en los Sistemas de Gestión del RENIEC; así como los lineamientos para la determinación, implementación, tratamiento, seguimiento de las acciones correctivas, observaciones y oportunidades de mejora, que son resultado de las auditorías internas/externas, resultado de la revisión por la Alta Dirección, resultado de análisis de los indicadores del Sistema de Gestión, eventos e incidentes de Seguridad de la Información, así también define los lineamientos para controlar y dar seguimiento a las acciones correctivas necesarias para evitar que se repita la no conformidad.

11.2 Mejora Continua

El SGSI del proceso de Certificación Digital está implementado siguiendo los lineamientos establecidos en la Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información - Requisitos, que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información según el enfoque de mejora continua Ciclo de Deming: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).

En adición a lo descrito en el acápite anterior, la GRCD, implementa mejoras a sus procesos y controles de Seguridad de la Información mediante la propuesta de mejoras provenientes de:

- Reuniones de los responsables de los sub procesos, Gestor Líder y/o Gestor Operativo del SGSI.
- Los resultados de las acciones para tratar riesgos y oportunidades de Seguridad de la Información.
- Los resultados de las Revisiones por la Alta Dirección.
- Los resultados de las auditorías internas/externas de seguridad de la información.
- Los resultados de las acciones correctivas que incluyen acciones de mejora.

XII. VIGENCIA

Entrará en vigencia a partir de su aprobación.

XIII. APROBACIÓN

Será aprobada mediante Resolución Secretarial.

XIV. ANEXOS

ANEXO N° 01

MATRIZ DE EXPECTATIVAS Y NECESIDADES DE LAS PARTES INTERESADAS RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN

MATRIZ DE EXPECTATIVAS Y NECESIDADES DE LAS PARTES INTERESADAS RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN					
Proceso Clave o Misional	**Sub Proceso**	**Grupo de Interés**	**Requisitos**	**Expectativas y Necesidades**	**Estrategia**
Certificación Digital	Gestión ECERNEP	• EREP • Cliente Ciudadano • Sector Público • Sector Privado • AAC (INDECOPI) • Aliados Estratégicos	• Acceso a la información. • Información correcta. • Información oportuna. • Cumplimiento de la Normativa.	• Confidencialidad de la Información. • Integridad de la Información • Disponibilidad de la Información	Implementación de un Sistema de Gestión de Seguridad de la Información bajo la Norma ISO/IEC 27001:2013.
	Producción del Certificado Digital y Prestación de Servicios (ECEP)				

ANEXO N° 02

MATRIZ DE REQUISITOS DE COMPETENCIA PARA EL SGSI

MATRIZ DE REQUISITOS DE COMPETENCIA PARA EL SGSI														
UNIDAD ORGANICA		xxxxx											Fecha Actualización:	xx/xx/xx
N°	Roles	Educación			Formación / con especialidad en alguno de los siguientes temas o una combinación de estos							Experiencia Laboral en años		Otras competencias + habilidades o destrezas
		Estudios Técnicos	Estudios Universitarios	Secundaria Completa	Derecho	Economía	Ingeniería	Administración	Computación e Informática	Contabilidad	Otras Carreras	Laboral Total	En la Actividad a realizar	

Nota: Orientación para el uso de la matriz de competencia:

1. Para campo Educación:
   a) La educación está referida al tipo de estudios realizados por el trabajador, se demuestra con la presentación de certificado o constancia.
   b) Se podrá marcar más de un casillero, en cuyo caso la interpretación será la siguiente: "El trabajador puede tener cualquiera de los tipos de educación marcada".
2. Para campo de Formación:
   a) La formación esta referida a la orientación de los conocimientos recibidos por el trabajador. Se demuestra con la presentación de certificados o constancias.
   b) Se podrá marcar más de un casillero, en cuyo caso la interpretación será la siguiente: "El trabajador puede tener cualquiera de los tipos de formación marcada".
3. Para campo de Experiencia:
   a) La experiencia referida a la relación laboral que demuestre haber tenido el trabajador. Se demuestra con la presentación de certificados o constancias.
   b) Se podrá especificar / detallar más de un casillero, en cuyo caso la interpretación será la siguiente: "El trabajador debe cumplir los requisitos especificados en cada casillero llenado".
4. Para campo de Competencias:
   a) Habilidades del personal nuevo: Se solicitará a la Gerencia de Talento Humano se realice una evaluación psicológica durate el proceso de selección de personal.
   b) Habilidades del personal que labora en el SGSI de la GRCD serán evaluadas a través de la evaluación de desempeño de acuerdo a la Directiva DI-412-GTH/011 "Gestión del Rendimiento" a cargo de la Gerencia de Talento Humano, seleccionándose 5 competencias según el tipo de rol a evaluar.

ANEXO N° 03

MATRIZ DE PLANIFICACIÓN Y SEGUIMIENTO DE OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

MATRIZ DE PLANIFICACIÓN Y SEGUIMIENTO DE OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

GESTION DEL RIESGO							
OBJETIVO GENERAL DE SEGURIDAD DE LA INFORMACIÓN	OBJETIVO ESPECIFICO DE SEGURIDAD DE LA INFORMACIÓN	ACTIVIDAD	RESPONSABLE	Fecha Inicio	Fecha Fin	ESTADO	OBSERVACIONES

Elaborado por:	Revisado por:	Aprobado por:
Fecha:	Fecha:	Fecha:

ANEXO N° 04

LISTA DE DISTRIBUCIÓN DE DOCUMENTOS

CODIGO - NOMBRE DEL DOCUMENTO. VERSIÓN				
Copia Controlada N°	**Función del usuario responsable**	**Nombre del usuario responsable**	**Firma**	**Fecha de Recepción**

ANEXO N° 05

ACTA DE ELIMINACIÓN

De acuerdo con lo dispuesto en el Manual de Seguridad de la Información vigente, habiéndose aprobado la _____ versión del documento normativo _____, y con la finalidad de evitar el uso equivocado de documentos obsoletos, se ha recuperado y eliminado la Copia Controlada N°_____ correspondiente a la _____ versión del referido documento normativo, entregada a _____ el ____/_____/_____.

Fecha: _____/_____/_____

Responsable del Sub Proceso	Gestor Operativo de Seguridad de la Información
Nombre:	Nombre:
DNI N°:	DNI N°:

ANEXO N° 06

INVENTARIO DE DOCUMENTOS

Fecha de actualización			Unidad Orgánica			
Código	Tipo de documento (Manual; Directiva; Guía de Procedimientos; NAI, Doc. Técnico)	Nombre del documento	Versión Vigente	Documento que aprueba	Fecha de aprobación	Responsable de la distribución

ANEXO N° 07

FICHA DE INDICADOR

(Ejemplo de aplicación de la ficha de indicador)

RESULTADO DEL INDICADOR PCD_003

Nombre del Indicador	Porcentaje de implementacion de actividades del PTR	Fórmula del Indicador	Cantidad de actividades ejecutadas del PTR / Cantidad de actividades planificadas del PTR * 100

Descripción	Periodo de Evaluación											
	jul-17	ago-17	sep-17	oct-17	nov-17	dic-17	ene-18	feb-18	mar-18	abr-18	may-18	jun-18
Meta	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%
Resultado del Indicador	100%	100%	100%	100%	100%	100%	100%	100%				
Limite Superior (Bueno)	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%	95%
Limite Inferior (Malo)	90%	90%	90%	90%	90%	90%	90%	90%	90%	90%	90%	90%
Numerador	3	3	3	3	1	1	1	1				
Denominador	3	3	3	3	1	1	1	1