MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

"PROCESO DE ASESORAMIENTO EN LA GESTIÓN DE LA CALIDAD E INNOVACIÓN"

RESOLUCIÓN SECRETARIAL N° 159 2019-SGEN/RENIEC		
MGSI-205-GCI/001	VERSIÓN: 01 N° PÁGINAS: 41	FECHA DE APROBACIÓN: 02 JUL. 2019

Capítulo	Título
VIII	**OPERACIÓN**
8.1	Planificación y control operacional
8.2	Evaluación de riesgos de seguridad de la información
8.3	Tratamiento de riesgos de seguridad de la información
IX	**EVALUACION DE DESEMPEÑO**
9.1	Monitoreo, medición, análisis y evaluación
9.2	Auditoría Interna
9.3	Revisión por la Gerencia
X	**MEJORAS**
10.1	No conformidades y acciones correctiva
10.2	Mejora continua
XI	**VIGENCIA**
XII	**APROBACIÓN**
XIII	**ANEXOS**
Anexo N° 01	Matriz de Expectativas y Necesidades de las Partes Interesadas (Referencia: Numeral 4.2)
Anexo N° 02	Formato para "Lista de Contactos Externos" (Referencia: Numeral 5.3.5)
Anexo N° 03	Matriz de Planificación y Seguimiento de Objetivos de Seguridad de la Información (Referencia: Numeral 6.2)
Anexo N° 04	Matriz de requisitos de competencias para los roles del Sistema de Gestión de Seguridad de la Información (SGSI) del "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación". (Referencia: Numeral 7.2)
Anexo N° 05	Lista maestra de documentos (Referencia: Numeral 7.5.1)
Anexo N° 06	Lista de Distribución de Documentos (Referencia: Numeral 7.5.1)
Anexo N° 07	Acta de Eliminación (Referencia: Numeral 7.5.1)
Anexo N° 08	Sistema de Gestión de Seguridad de la Información - SGSI Cuadro de Mando Operativo – CMO (Referencia: Numeral 9.1)

I. OBJETO Y CAMPO DE APLICACIÓN

Especificar los elementos principales del Sistema de Gestión de Seguridad de la Información del "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación" del Registro Nacional de Identificación y Estado Civil en adelante 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 Calidad e Innovación ha sido diseñado de acuerdo a lo establecido en los siguientes documentos:

2.1 La Resolución Comisión de Normalización y de Fiscalización de barreras comerciales no arancelarias N° 129-2014/CNB-INDECOPI, que aprueba 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. Reemplaza a la NTP-ISO/IEC 27001:2008 [revisada el 2013], del 20 de noviembre del 2014.

2.2 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".

2.3 La Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 "TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información: Requisitos. 2ª Edición en todas las entidades del Sistema Nacional de Informática, del 08 de enero de 2016.

2.4 La Resolución Ministerial N° 0166-2017-PCM, que modifica el artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información, del 20 de junio de 2016.

III. TÉRMINOS Y DEFINICIONES

Las definiciones de los términos relacionados a la gestión de seguridad de la información que se ha utilizado en este documento se encuentran 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". Asimismo, se ha hecho uso de las siguientes siglas:

SIGLA	NOMBRE
CGSI	Comité de Gestión de Seguridad de la Información
CIGSI	Comité Interno de Gestión de Seguridad de la Información
GCI	Gerencia de Calidad e Innovación
GPP	Gerencia de Planificación y Presupuesto
ISO	International Organization for Standarization

SIGLA	NOMBRE
OSDN	Oficina de Seguridad y Defensa Nacional
POI	Plan Operativo Institucional
RENIEC	Registro Nacional de Identificación y Estado Civil
ROF	Reglamento de Organización y Funciones
SGC	Sub Gerencia de Calidad
SGGP	Sub Gerencia de Gestión por Proyectos
SGI	Sub Gerencia de Innovación

IV. CONTEXTO DE LA ORGANIZACIÓN

4.1 De la organización y su contexto

4.1.1 Registro Nacional de Identificación y Estado Civil (RENIEC)

El Registro Nacional de Identificación y Estado Civil – 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 N° 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.

El Registro Nacional de Identificación y Estado Civil – 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 clave, procesos estratégicos y procesos de soporte, como se aprecia en el Mapa de Procesos que se muestra.

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

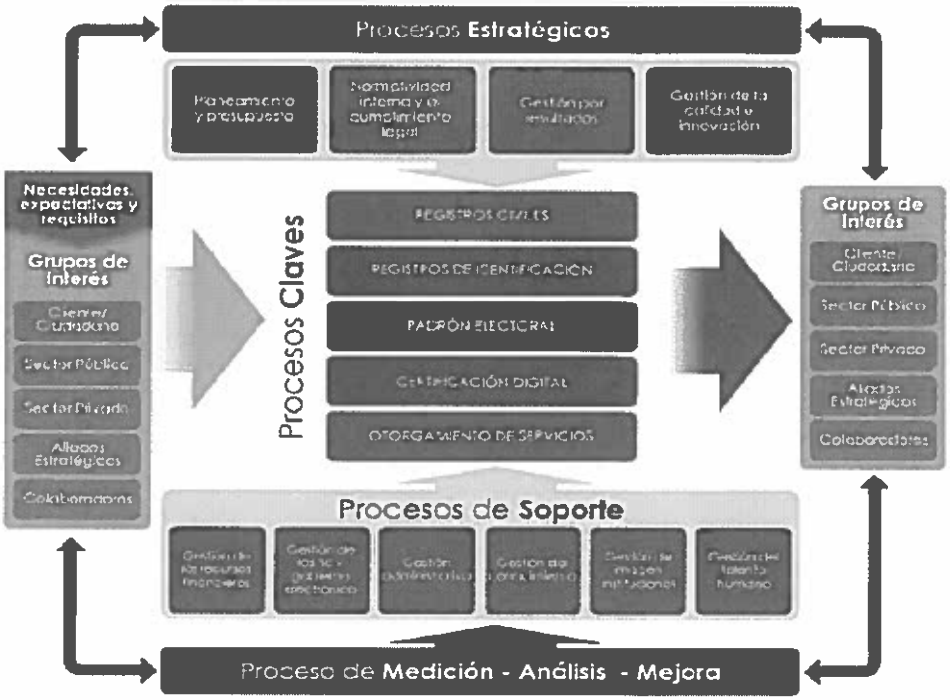

FIGURA N° 01: MAPA DE PROCESOS DEL RENIEC

Fuente referencial: Resolución Jefatural N° 0166-2015/JNAC/RENIEC (14JUL2015)

El Plan Estratégico Institucional vigente1 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

"Ciudadanos identificados con acceso a servicios amigables e innovadores en tiempo real, integrados digitalmente a través de la entidad del registro del Estado Peruano que garantiza su identidad y seguridad jurídica, y que contribuye a la modernización del Estado y al desarrollo del país".

El RENIEC hace uso intensivo de las tecnologías de la información que soportan todos sus procesos de negocio, permitiendo de esta

[1] Con Resolución Jefatural N°124-2018/JNAC/RENIEC de fecha 24 de octubre del 2018, se aprueba el Plan Estratégico Institucional 2018-2020.

manera el logro de los objetivos estratégicos y el cumplimiento de su Misión y Visión.

El RENIEC, en el Reglamento de Organización y Funciones, Artículo 10° incisos j); k); p); y q); define funciones asociadas 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.

Con la implementación del Sistema de Gestión de Seguridad de la Información, 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 de los clientes (persona natural y jurídica), el RENIEC da cumplimiento a lo dispuesto por la Resolución Ministerial 004-2016-PCM, en relación al uso de la referida norma.

Mediante Resolución Jefatural N° 073-2016/JNAC/RENIEC del 01 junio de 2016, 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.

4.1.2 Dueño de Proceso de Asesoramiento en la Gestión de la Calidad e Innovación

La Gerencia de Calidad e Innovación es el Órgano de asesoramiento encargado de definir, implementar, controlar y supervisar las políticas, mecanismos, roles y responsabilidades de los sistemas de gestión calidad del Registro Nacional de Identificación y Estado Civil - RENIEC, así como investigar, evaluar y promover iniciativas de innovación que provengan de las distintas áreas de la institución o de sus propias investigaciones. Asimismo, asesora y brinda asistencia técnica en la gestión por proyectos para los planes, programas, proyectos y actividades para el fortalecimiento institucional De acuerdo al Reglamento de Organización y Funciones vigente, hay tres (03) sub gerencias adscritas a la Gerencia de Calidad e Innovación.

FIGURA N° 02: ORGANIGRAMA GERENCIA DE CALIDAD E INNOVACION
Fuente: Reglamento de Organización y Funciones (ROF)

Las funciones de cada unidad orgánica se encuentran descritas en el Reglamento de Organización y Funciones2.

PROCESOS	ORGANO			
	GCI	SGC	SGGP	SGI
Despliegue de la Arquitectura Institucional	X	X	X	X
Formulación y Evaluación de Inversión	X		X	X
Promoción de la Generación del Perfil Distintivo RENIEC	X		X	
Actualización del Portafolio de Proyectos e Iniciativas RENIEC			X	
Promoción de la Cultura en Gestión de Proyectos			X	
Acompañamiento a la Gestión del Proyecto RENIEC			X	
Asesoría al Gobierno de Procesos RENIEC		X		
Seguimiento y Mejora de Sistemas de Gestión		X		
Inducción en Herramientas y Técnicas de Documentación de Procesos		X		
Asesoramiento a la Gestión de Retos				X
Generación de Capacidades de Innovación				X
Vigilancia Tecnológica				X

2 Aprobado mediante Resolución Jefatural N°073-2016/JNAC/RENIEC, de fecha 01 de junio de 2016 y su modificatoria.

La secuencia e interacción de los procesos de realización se encuentra definida en el siguiente Mapa de Procesos:

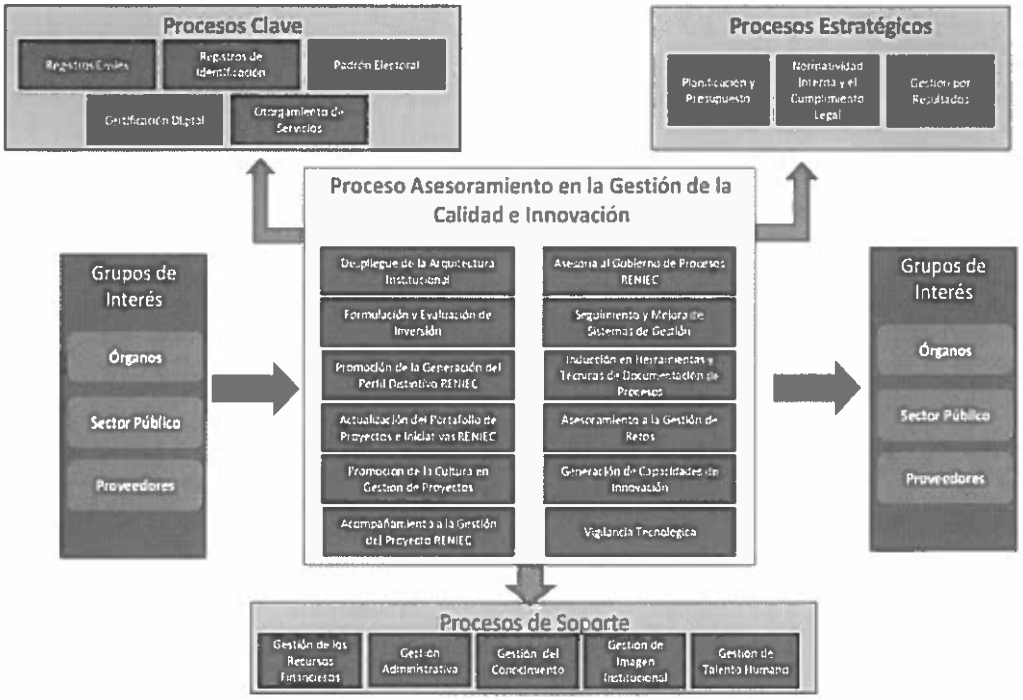

FIGURA N° 03: MAPA DE PROCESO: ASESORAMIENTO EN LA GESTION DE LA CALIDAD E INNOVACIÓN
Fuente: Proyecto de Ingeniería de procesos RENIEC

4.2 De las necesidades y expectativas de las partes interesadas

El Sistema de Gestión de Seguridad de la Información ha identificado a las partes interesadas del "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación", así como sus necesidades y expectativas. Se mantiene información documentada al respecto, para cuyo efecto se ha diseñado el formato que se aprecia en el **Anexo N° 01 "Matriz de Expectativas y Necesidades de las Partes Interesadas".**

4.3 Alcance del Sistema de Gestión de Seguridad de la Información

El alcance del Sistema de Gestión de Seguridad de la Información del "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación" a cargo de la Gerencia de Calidad e Innovación (GCI), comprende la asesoría y asistencia técnica en la implementación de los sistemas de gestión, gestión de la innovación, gestión por procesos y gestión por proyectos para

los planes, portafolios y actividades que contribuyan al fortalecimiento de la institución, generados a través de uno o varios de los siguientes procesos:

1. Despliegue de la Arquitectura Institucional
2. Formulación y Evaluación de Inversión
3. Promoción de la Generación del Perfil Distintivo RENIEC
4. Actualización del Portafolio de Proyectos e Iniciativas RENIEC
5. Promoción de la Cultura en Gestión de Proyectos
6. Acompañamiento a la Gestión del Proyecto RENIEC
7. Asesoría al Gobierno de Procesos RENIEC
8. Seguimiento y Mejora de Sistemas de Gestión
9. Inducción en Herramientas y Técnicas de Documentación de Procesos
10. Asesoramiento a la Gestión de Retos
11. Generación de Capacidades de Innovación
12. Vigilancia Tecnológica

El Sistema de Gestión de Seguridad de la Información, cubrirá los procesos y activos de información en las siguientes ubicaciones físicas:

PROCESO	UUOO	SEDE	DOMICILIO	UBICACIÓN FÍSICA
1. Despliegue de la Arquitectura Institucional	GCI	Administrativa	Jr. Bolivia 109, Cercado de Lima	Piso 33
2. Formulación y Evaluación de Inversión	GCI	Administrativa	Jr. Bolivia 109, Cercado de Lima	Piso 33
3. Promoción de la Generación del Perfil Distintivo RENIEC	GCI	Administrativa	Jr. Bolivia 109, Cercado de Lima	Piso 33
4. Actualización del Portafolio de Proyectos e Iniciativas RENIEC	SGGP	Administrativa	Jr. Bolivia 109, Cercado de Lima	Piso 33
5. Promoción de la Cultura en Gestión de Proyectos	SGGP	Administrativa	Jr. Bolivia 109, Cercado de Lima	Piso 33
6. Acompañamiento a la Gestión del Proyecto RENIEC	SGGP	Administrativa	Jr. Bolivia 109, Cercado de Lima	Piso 33
7. Asesoría al Gobierno de Procesos RENIEC	SGC	Administrativa	Jr. Bolivia 109, Cercado de Lima	Piso 33
8. Seguimiento y Mejora de Sistemas de Gestión	SGC	Administrativa	Jr. Bolivia 109, Cercado de Lima	Piso 33
9. Inducción en Herramientas y Técnicas de Documentación de Procesos	SGC	Administrativa	Jr. Bolivia 109, Cercado de Lima	Piso 33
10. Asesoramiento a la Gestión de Retos	SGI	Administrativa	Jr. Bolivia 109, Cercado de Lima	Piso 33
11. Generación de Capacidades de Innovación	SGI	Administrativa	Jr. Bolivia 109, Cercado de Lima	Piso 33
12.Vigilancia Tecnológica	SGI	Administrativa	Jr. Bolivia 109, Cercado de Lima	Piso 33

4.4 Sistema de Gestión de Seguridad de la Información

La Alta Dirección ha establecido, documentado y mantiene un Sistema de Gestión de Seguridad de la Información 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. 2ª. Edición".

Con base al modelo del ciclo de Deming, los capítulos "Contexto de la organización", "Liderazgo", "Planificación" y "Soporte" del presente manual corresponden a la descripción del componente "Planear", el capítulo "Operación" corresponde a la descripción del componente "Hacer", el capítulo "Evaluación de desempeño" corresponde a la descripción del componente "Verificar" y finalmente, el capítulo "Mejoras" corresponde a la descripción del componente "Actuar".

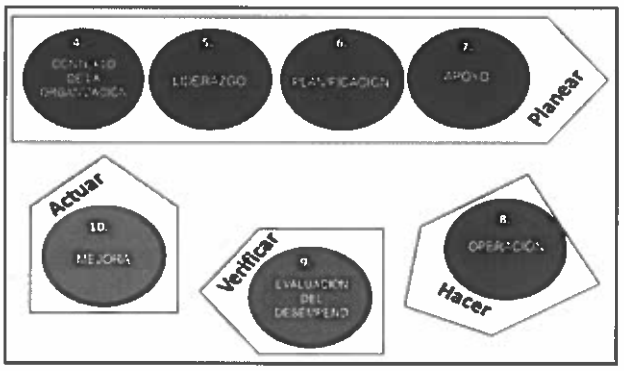

FIGURA N° 04: CICLO DE DEMING
Fuente: Ciclo de Mejora Continua de Edwards Deming

V. LIDERAZGO

5.1 Liderazgo y compromiso

La Alta Dirección evidencia su liderazgo y compromiso con el desarrollo e implementación del Sistema de Gestión de Seguridad de la Información del "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación" a través de las actividades que se describen:

COMPROMISO	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.	• Plan Estratégico Institucional. • Plan Operativo Institucional de la Oficina de Seguridad y Defensa Nacional define en sus objetivos, la implementación del Sistema de Gestión de Seguridad de la Información en los procesos claves y de asesoría del RENIEC. • Reglamento de Organización y Funciones, donde se formaliza la estructura orgánica de la entidad orientada al esfuerzo institucional para alcanzar al logro de su misión, visión y objetivos.
Asegurando la integración de los requisitos del Sistema de Gestión de la Seguridad de la	• El RENIEC tiene Sistemas de Gestión de Seguridad de la Información en los procesos clave de

COMPROMISO	EVIDENCIAS
Información a los procesos de la organización.	la institución: - Certificación Digital - Registros de Identificación. - Registros Civiles. - Padrón Electoral. Así también tiene el SGSI en los procesos de soporte: - Gestión de las TIC's y Gobierno Electrónico. • Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información, en cumplimiento 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". • Documento de gestión dirigido a los responsables de los Sub Procesos indicando que deben incluir el cumplimiento de los requerimientos de Seguridad de la Información en los documentos normativos. • Documento de Declaración de Aplicabilidad de la OSDN, en cumplimiento de la DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información".
Asegurando la disponibilidad de los recursos necesarios para el sistema de gestión de seguridad de la información.	• El RENIEC a través de la Gerencia de Planificación y Presupuesto, formula el PIA con los órganos en el cual se considera la asignación de presupuesto para el mantenimiento del Sistema de Gestión de Seguridad de la Información de los procesos certificados (auditorías externas, cursos y controles de seguridad).
Asegurando que los Sistemas de Gestión de Seguridad de la Información logren los resultados esperados.	• Resolución Jefatural N° 069-2017/JNAC (22MAY2017) mediante la que se reconstituye el Comité de Gestión de Seguridad de la Información del Registro Nacional de Identificación y Estado Civil en

COMPROMISO	EVIDENCIAS
	cumplimiento de la Resolución Ministerial N° 004-2016-PCM (08ENE2016). • La Oficina de Seguridad y Defensa Nacional (OSDN), a través de la Sub Gerencia de Seguridad de la Información, como órgano líder en la implementación del Sistema de Gestión de Seguridad de la Información en el "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación", asesora al Comité Interno de Gestión de Seguridad de la Información, para establecer los indicadores base para la medición del cumplimiento de los objetivos de seguridad de la información.
Fortaleciendo las competencias de los servidores del RENIEC para que contribuyan a la efectividad del Sistema de Gestión de Seguridad de la Información.	• Revisiones de la Alta Dirección. • Plan de Desarrollo de Personas (PdP), ejecutado por la Escuela Registral (ER) en coordinación con la OSDN, quien formula los temas de capacitación en materia de seguridad de la información.
Promoviendo la mejora continua	• La implementación del Sistema de Gestión de Seguridad de la Información en la GCI, implica una gestión de mejora continua, ya que está basado en el modelo de gestión de procesos de Deming: Planificar-Hacer-Verificar-Actuar (PHVA). • Documentos normativos: Directiva Gestión por Procesos del RENIEC DI- 366-GCI/007, Directiva de Tratamiento de Hallazgos DI-421-GCI/012, Guía de Procedimientos Mejora de Procesos del RENIEC GP-378-GCI/001 y Guía de Procedimientos Metodología de documentación de Procesos del RENIEC GP-379-GCI/002.
Apoyando los roles de Gestión relevantes para demostrar su liderazgo según corresponda a sus áreas de responsabilidad.	• Artículo 38° del Reglamento de Organización y Funciones vigente, mediante el cual el RENIEC empodera a la Oficina de Seguridad y Defensa Nacional para liderar la

COMPROMISO	EVIDENCIAS
	implementación de la Seguridad de la Información a nivel institucional. • Memorandos de asignación de roles de Gestores Líderes y Operativos para el tratamiento de la Seguridad de la Información, emitidos por la Gerencia de Calidad e Innovación. • La OSDN es integrante del Comité de Gestión de Seguridad de la Información.

5.2 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, y es como sigue:

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. Es adecuada a las necesidades de la organización y de los clientes.
b. Incluye el compromiso para satisfacer los requisitos y para la mejora continua.
c. Proporciona 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 http://intranet.reniec.gob.pe.
   - Publicación en periódico mural y/o lugares visibles.
   - Presentándola en reuniones a los trabajadores
   - Charlas de sensibilización a los trabajadores.

- Revisando su cumplimiento durante las auditorías internas del Sistema de Gestión de Seguridad de la Información.
- Sistema Integrado de Trámite Documentario

e. Sea revisada durante la Revisión por la Gerencia, para su continua adecuación y eficacia

5.3 Roles, responsabilidades y autoridades organizacionales

Los roles, responsabilidades y autoridades para los diferentes órganos y unidades orgánicas del Sistema de Gestión de Seguridad de la Información son definidas y comunicadas por la Oficina de Seguridad y Defensa Nacional.

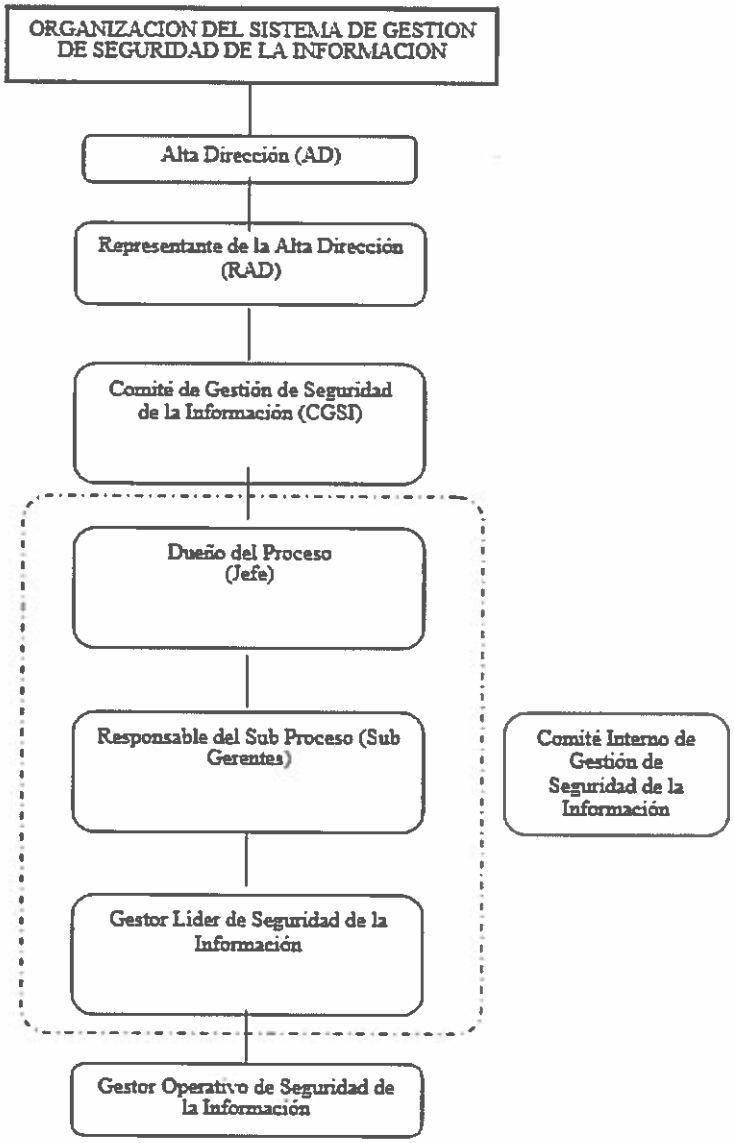

FIGURA N° 05: ORGANIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

5.3.1 Alta Dirección

Constituye el máximo nivel de conducción y decisión del RENIEC. Está conformado por la Jefatura Nacional, la Gerencia General, la Secretaría General, la Oficina de Seguridad y Defensa Nacional, la Defensoría de la Identidad, el Gabinete de Asesores, el Consejo Técnico y el Consejo Consultivo, siendo sus principales responsabilidades:

- Formular, revisar y aprobar la Política de Seguridad de la Información.
- Proporcionar los recursos necesarios para la seguridad de la información.
- Asegurar que los controles y oportunidades de seguridad de la información sean implementados y de conocimiento si es necesario de toda la organización.

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

Es el máximo órgano consultivo sobre la seguridad de la información, encargado de impulsar la implementación, operación, monitoreo, revisión, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información en el RENIEC.

Está constituido mediante Resolución Jefatural N° 0069-2017/JNAC/RENIEC, que aprueba la reconstitución del Comité de Gestión de Seguridad de la Información, el mismo que está integrado por los siguientes miembros:

N°	REPRESENTANTE	CARGO
1	Jefe Nacional o su representante.	Presidente
2	Jefe de la OSDN o quien haga sus veces.	Secretario Técnico
3	Gerente de Administración o quien haga sus veces.	Miembro
4	Gerente de Planificación y Presupuesto o quien haga sus veces.	Miembro
5	Gerente de Tecnología de la Información o quien haga sus veces.	Miembro
6	Gerente de Asesoría Jurídica o quien haga sus veces.	Miembro
7	Oficial de Seguridad de la Información.	Miembro
8	Un representante de Gabinete de Asesores de la JNAC.	Miembro

El CGSI se encargará de las siguientes funciones:

- 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.
- Promover y gestionar la implementación Sistema de Gestión de Seguridad de la Información.
- Promover la gestión de seguridad de la información, en los procesos y cultura organizacional.
- Gestionar la asignación de personal y recursos necesarios para la implementación del Sistema de Gestión de Seguridad de la Información.
- 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.
- Evaluar el desempeño del Sistema de Gestión de Seguridad de la Información.
- Otras funciones que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia.

5.3.3 Oficina de Seguridad y Defensa Nacional (OSDN)

Son funciones específicas de la OSDN en relación a la seguridad de la información:

- Coordinar con la Gerencia de Planificación y Presupuesto a través de la Secretaría General la articulación de la Política de Seguridad y Defensa Nacional con el Plan Estratégico Institucional – PEI.
- Conducir la implementación del Sistema de Gestión de Seguridad de la Información en la institución de acuerdo a la normatividad vigente, en el ámbito de su competencia.
- Informar a la Jefatura Nacional la situación institucional en materia de seguridad de la información.
- Desarrollar, en el ámbito de su competencia, las acciones orientadas a implementar el funcionamiento del Sistema de Seguridad de la Información de acuerdo con los lineamientos establecidos por la Alta Dirección y las normas legales pertinentes.
- Coordinar con la Gerencia General y la Gerencia de Tecnología de la Información las acciones de implementación, desarrollo y cumplimiento de las disposiciones vigentes sobre la seguridad de la información.
- Promover la difusión de la Seguridad de la Información en coordinación con la Alta Dirección y la Escuela Registral.

5.3.4 Sub Gerencia de Seguridad de la Información(OSDN/SGSI)

La OSDN/SGSI, es la unidad orgánica encargada de la gestión del sistema de seguridad de la información del RENIEC, responsable de desarrollar e implantar un sistema de gestión de la seguridad que permita identificar y dar respuesta a los nuevos riesgos de la institución.

Son funciones específicas de la Sub Gerencia de Seguridad de la Información:

- Proponer las políticas, planes, programas y actividades relacionadas al Sistema de Gestión de Seguridad de la Información, para reducir los riesgos que afecten la confidencialidad, integridad y disponibilidad de la información en los procesos institucionales.
- Establecer, implementar, monitorear, revisar y mejorar el Sistema de Gestión de Seguridad de la Información en el RENIEC, en el cumplimiento del marco legal vigente y estándares internacionales.
- Planear, organizar, programar, ejecutar y supervisar las acciones de Seguridad de la Información de acuerdo a la normatividad vigente y estándares internacionales.
- Formular, supervisar y monitorear la implementación del Plan de Seguridad de la Información del RENIEC, garantizando su correcta ejecución en el cumplimiento del marco legal vigente y estándares internacionales.
- Proponer mejoras o iniciativas en materia de seguridad de la información al Equipo de Gestión o al Oficial de Seguridad de la información en materia de gestión de riesgos, activos de información, procesamiento de la información, mejoras al Sistema de Gestión de Seguridad de la Información (SGSI), entre otros.
- Definir una metodología de evaluación de riesgos apropiada para el Sistema de Gestión de Seguridad de la Información y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable.
- Administrar el desarrollo y la aplicación de las políticas de seguridad, normas y procedimientos para garantizar el mantenimiento continuo de la seguridad de la información y la protección de activos.
- Coordinar con la Gerencia General, Secretaría General, Gerencia de Tecnología de la Información y sus áreas la implementación de las políticas, normativas y controles para reducir los riesgos de seguridad de la información en la institución.
- Supervisar las áreas respecto a la implementación de los controles de seguridad de la información en el ámbito de su competencia.

- Capacitar y sensibilizar al personal frente a la cultura de seguridad en toda la institución.
- Gestionar mejoras a nivel de procedimientos y aplicaciones informáticas utilizadas dentro del ámbito de su competencia.
- Las demás funciones que se le asignen en el marco de su competencia.

5.3.5 Oficial de Seguridad de la Información

Es el responsable de coordinar la implementación del Sistema de Gestión de Seguridad de la Información en el RENIEC.

5.3.6 Comité Interno de Gestión de Seguridad de la Información (CIGSI)[3]

Es la instancia permanente a nivel interno, de carácter no técnico sobre la seguridad de la información en el área que se implementa el SGSI; encargado de gestionar las actividades relevantes para establecer, implementar, monitorear, revisar y mejorar el SGSI.

Está integrado por los siguientes miembros:

N°	REPRESENTANTE	CARGO
1	Gerente de Calidad e Innovación	Presidente
2	Gestor Líder de Seguridad de la Información del "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación"	Secretario Técnico
3	Sub Gerentes de la Gerencia de Calidad e Innovación	Miembros

El CIGSI se encargará de las siguientes funciones:

- Asegurar que el Sistema de Gestión de Seguridad de la Información, se ejecute conforme a los requisitos de la normatividad vigente.
- Asegurar la integración de los requisitos del Sistema de Gestión de Seguridad de la Información en los procesos de la GCI.
- Revisar y aprobar la documentación que sea requisito normativo del Sistema de Gestión de Seguridad de la Información.
- Revisar y aprobar los resultados del proceso de gestión de riesgos seguridad de la Información.

3 Referencia Directiva DI-373-OSDN/007 Aprobada con Resolución Jefatural N° 004-2015/ GCI/ RENIEC de Fecha 28 de agosto de 2015. (IV. DEFINICIÓN DE TÉRMINOS – 4.2 COMITÉ INTERNO DE SEGURIDAD DE LA INFORMACIÓN).

- Establecer los objetivos específicos de seguridad de la información del área y la planificación para lograrlos, concordantes a 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.
- Revisar y aprobar las competencias de seguridad de la información en el marco de los roles requeridos para la implementación del Sistema de Gestión de Seguridad de la Información.
- Comunicar al 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 Sistema de Gestión de Seguridad de la Información.
- Gestionar la programación de las auditorías interna/externa del SGSI en coordinación con la GCI y las unidades orgánicas certificadas.
- Actualizar y difundir la Lista de Contactos con Autoridades en el marco del SGSI. Ver Anexo N° 02 Formato de "Lista de Contactos Externos"
- Revisar y evaluar los resultados del Sistema de Gestión de Seguridad de la Información, 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 Sistema de Gestión de Seguridad de la Información.
- Otras funciones que se le asigne en el ámbito de la competencia del SGSI.

5.3.7 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.

5.3.8 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.

5.3.9 Gestor Líder de Seguridad de la Información

La Oficina de Seguridad y Defensa Nacional asigna a los Gestores Líderes los roles, responsabilidades y autoridad para:

- Velar por el cumplimiento de la Política de Seguridad de la Información, documentos, directivas y normas relacionadas.
- Gestionar la asignación de recursos necesarios para el SGSI.

- Liderar y constituir el equipo de riesgos de Seguridad de la Información y la elaboración de la Declaración de Aplicabilidad.
- Monitorear la ejecución del Plan de Tratamiento de Seguridad de la Información.
- Liderar y promover la ejecución de planes de sensibilización de Seguridad de la Información.
- Planificar y monitorear la evaluación de desempeño del SGSI a través de los indicadores de gestión.
- Informar al Sub Gerente de Seguridad de la Información de la Oficina de Seguridad y Defensa Nacional, sobre el desempeño y oportunidades de mejora del Sistema de Gestión de Seguridad de la Información.
- Liderar las actividades para la planificación y ejecución de las auditorías internas/externas del SGSI.
- Monitorear el cierre de las no conformidades y las acciones correctivas.
- Dirigir las acciones para la clasificación de la información, etiquetado y uso adecuado de los activos de información y la gestión de vulnerabilidades, eventos e incidentes de Seguridad de la Información.
- Otras funciones que se le asigne en el ámbito de su competencia.

5.3.10 Equipo de Riesgos

Es el grupo multifuncional conformado por el Gestor(es) Líder(es) y Operativo(s) de Seguridad de la Información del "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación". Sus funciones son:

- Elaborar el inventario de activos de información.
- Realizar la identificación, análisis y 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 EGSI, el informe de la identificación, análisis evaluación y tratamiento de los riesgos y oportunidades del SGSI.
- Otras funciones que se le asigne en el ámbito de su competencia

5.3.11 Gestor Operativo de Seguridad de la Información

Los Responsables de los sub procesos designan a los Gestores Operativos y les asigna, roles, responsabilidades y autoridad para:

- Integrar el Equipo de Riesgos y ejecutar las actividades que demande la Gestión de Riesgos de Seguridad de la Información.

- Elaborar la Declaración de Aplicabilidad en concordancia con el Plan de Tratamientos de Riesgos y Oportunidades de Seguridad de la Información.
- Ejecutar los planes de sensibilización en Seguridad de la Información.
- Conservar la información documentada necesaria por el Sistema de Gestión de Seguridad de la Información.
- Ejecutar y/o gestionar las acciones que demanden el Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información.
- Ejecutar la evaluación de desempeño del Sistema de Gestión de Seguridad de la Información a través de los indicadores de gestión.
- Participar activamente en 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 para que los activos de información estén debidamente inventariados, 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.

VI. PLANIFICACIÓN

6.1 Acciones para tratar los riesgos y las oportunidades

El RENIEC a través de la Directiva **DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información"** y el Instructivo **IN-208-OSDN/001 Gestión de Riesgos de Seguridad de la Información"**, establece los 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 Sistema de Gestión de Seguridad de la Información.

6.1.1 Generalidades

El Dueño del "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación":

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

b) Desarrolla acciones para la prevención o reducción de efectos indeseados, en coordinación con sus unidades orgánicas, con el fin de cumplir los objetivos y requisitos del Sistema de Gestión de Seguridad de la Información.

c) Promueve la mejora continua.

d) Identifica los riesgos y oportunidades de mejora para su tratamiento y seguimiento, aplicando la Directiva DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información".

e) Aplica las estrategias, controles y evaluación del riesgo residual esperado descritos en la Directiva DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información".

6.1.2 Valoración del Riesgo de Seguridad de la Información

Las actividades de identificación, análisis, evaluación y tratamiento de riesgos y oportunidades de seguridad de la información se encuentran definidas en la Directiva DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información" e INS-208-OSND/001 "Gestión de Riesgos de Seguridad de la Información", que establece los criterios contra los cuales se evalúan los riesgos y oportunidades de seguridad de la información, lineamientos para identificar, analizar, evaluar, y tratar los riesgos de seguridad de la información a los que se encuentra expuesto el Registro Nacional de Identificación y Estado Civil – RENIEC, hasta obtener un nivel aceptable del riesgo y garantizar la Seguridad de la Información en las áreas que cuenten o implementen un Sistema de Gestión de Seguridad de la Información.

El Dueño del "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación" y los Responsables de los sub procesos, a través de los Gestores Líderes y Operativos de Seguridad de la Información, han realizado la identificación riesgos y oportunidades, y posteriormente generando un "Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información", bajo los criterios de confidencialidad, integridad y disponibilidad de la información.

Se mantiene información documentada de este proceso.

6.1.3 Tratamiento de riesgo de seguridad de la información

Los lineamientos para tratar los riesgos del Sistema de Seguridad de la información se encuentran definidos en la Directiva DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información" e INS-208-OSND/001 "Gestión de Riesgos de Seguridad de la Información", que establecen estrategias, responsables y tiempo estimado, para el tratamiento del riesgo y oportunidades,

seleccionando los controles u oportunidades que sean necesarios hasta obtener un nivel aceptable del riesgo.

El Dueño del Proceso y los responsables de los sub procesos gestionan la implementación de los controles e impulsores definidos en el Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información e informan a la Sub Gerencia de Seguridad de la Información, cualquier cambio en el proceso, para realizar una re-evaluación del riesgo de seguridad de la información.

Se han establecido controles necesarios para el Sistema de Gestión de Seguridad de la Información de la OSDN, 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 Técnica Peruana NTP-ISO/IEC 27001:2014 "Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información: Requisitos".

6.1.4 Gestión de Incidentes de Seguridad de la Información

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

6.2 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° 124-2018-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.*

Asimismo, la Gerencia de Calidad e Innovación (Dueño del Proceso) 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 EN LA GERENCIA DE CALIDAD E INNOVACIÓN

- *Minimizar la ocurrencia de vulnerabilidades o eventos de seguridad de la información.*
- *Reducir las brechas en la pérdida de la confidencialidad, integridad y disponibilidad mediante la gestión de riesgos de seguridad de la información.*
- *Generar las competencias de los servidores civiles a fin de generar cultura organizacional respecto a la Seguridad de la Información.*
- *Asegurar el mantenimiento del Sistema de Gestión de Seguridad de la Información.*

El Dueño del "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación" comunica a los responsables de los sub procesos, los objetivos específicos de seguridad de la información para su estricto cumplimiento, y los indicadores para su medición. Asimismo 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"**

VII. SOPORTE

7.1 Recursos

Los Responsables de los sub procesos inmersos en la Asesoramiento en la Gestión de la Calidad e Innovación elaboran anualmente su 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 Sistema de Gestión de Seguridad de la Información de la Gerencia de Calidad e Innovación.

7.2 Competencias

La Gerencia de Calidad e Innovación (Dueño del Proceso), en coordinación con sus unidades orgánicas, determina las necesidades de competencia del personal que realiza actividades que afectan la conformidad de los requisitos del Sistema de Gestión de Seguridad de la Información, a través del presente Manual, y la Guía de Procedimientos **GP-414-ER/SGFC/001 "Formación y Capacitación de la Escuela Registral".**

Las competencias necesarias para desarrollar actividades específicas del "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación" que puedan afectar la seguridad de la información son definidas y registradas por los Responsables de dichas áreas, en el formato del **Anexo N° 04 "Matriz de requisitos de competencias para los roles del Sistema de Gestión de Seguridad de la Información (SGSI) del "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación".**

La administración y organización de los legajos del personal se rigen conforme a lo establecido en la **DI-406-GTH/007 "Administración del Legajo del Servidor Civil en el RENIEC"**. Todos los servidores civiles que laboran en la Gerencia Tecnología de la Información son responsables de remitir la documentación personal que asegure la actualización de sus legajos personales.

7.3 Concientización

La Oficina de Seguridad y Defensa Nacional determina las necesidades de formación y sensibilización en temas de seguridad de la información del personal del RENIEC, y coordina con la Escuela Registral la programación y ejecución de las mismas, incluyéndose esta información en el Plan de Desarrollo de las Personas.

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 documento normativo **RE-207-ER/001 Reglamento de la Escuela Registral.**

Adicionalmente, la Gerencia de Calidad e Innovación a través de los Gestores Líderes y Operativos de Seguridad de la Información, ejecuta actividades de concientización en materia de seguridad de la información.

7.4 Comunicación

El RENIEC cuenta con una estructura de comunicación interna moderna, ágil y flexible, que facilita la comunicación entre todos los niveles de la organización, la cual está descrita en la **Directiva DI-417-SGEN/010 "Gestión Documental de RENIEC".**

Los métodos formales para la elaboración, aprobación y difusión de documentos normativos están definidos en la **DI-200-GPP/001 "Lineamientos para la Formulación de los Documentos Normativos del RENIEC"**; adicionalmente, a fin de asegurar el uso efectivo de la información, se cuenta con la **GP-399-GAJ/SGSJ/004 "Sistematización de documentación y normatividad interna y externa del RENIEC".**

Asimismo, a fin de vincular a todos los miembros de los Sistemas de Gestión en todos los distintos niveles jerárquicos y áreas, mejorar el desempeño y fortalecer el sentimiento de pertenencia, se utilizan las siguientes herramientas de comunicación interna:

HERRAMIENTAS	TEMAS
• Reuniones de trabajo. • Mesas de trabajo. • Correo electrónico. • Videoconferencias. • Intranet RENIEC • Infoleg. • Fondos de pantalla. • Periódico mural.	• 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. • Cambios y mejoras en el SGSI. • Otros temas relevantes para la seguridad de la información.

7.5 Información documentada

7.5.1 Generalidades

El Sistema de Gestión de Seguridad de la Información de la GCI, incluye:

a) La información documentada requerida por la Norma Técnica Peruana NTP-ISO/IEC 27001:2014.

b) Información documentada establecida como necesaria para la efectividad del mismo.

7.5.2 Creación, actualización y control de la información documentada

El RENIEC, a través de la Directiva **DI-200-GPP/001 "Lineamientos para la Formulación de los Documentos Normativos del RENIEC"**, establece lineamientos para la formulación de los documentos normativos que regulan las disposiciones técnicas normativas de las áreas internas, administrada por la Gerencia de Planificación y Presupuesto a través de la Sub Gerencia de Racionalización y es de aplicación obligatoria para todas las áreas del RENIEC.

El Registro Nacional de Identificación y Estado Civil, a través de la Directiva **DI-200-GPP/001 "Lineamientos para la Formulación de los Documentos Normativos del RENIEC"**, establece lineamientos que orienten a las áreas del RENIEC en el proceso de formulación, aprobación publicación, difusión, implementación, revisión, actualización y derogación de los Documentos Normativos para "normalizar" sus procesos de gestión tanto operativa como administrativa con el propósito de construir un ordenamiento jurídico interno que sea coherente y estructurado a partir de preceptos normativos correctamente formulados que respondan a las necesidades de la entidad para poder brindar y garantizar de manera efectiva e integral un servicio y una atención de calidad que satisfaga al ciudadano; así como, las exigencias de los organismos rectores de los sistemas administrativos y sistemas funcionales que se aplican en el RENIEC.

El Dueño del Proceso, hará la difusión, almacenamiento, conservación, actualización, retención y disposición de la información documentada relacionada al cumplimiento del Sistema de Gestión de Seguridad de la Información, cuando sea necesario y según corresponda.

7.5.3 Información Documentada

7.5.3.1 Documentos normativos que apoyan al Sistema de Gestión de Seguridad de la Información

Los documentos que apoyan el Sistema de Gestión de Seguridad de la Información garantizan que éste cuente con los procedimientos necesarios para asegurar la mejora continua. Estos documentos se encuentran jerarquizados y clasificados según la estructura general que se muestra:

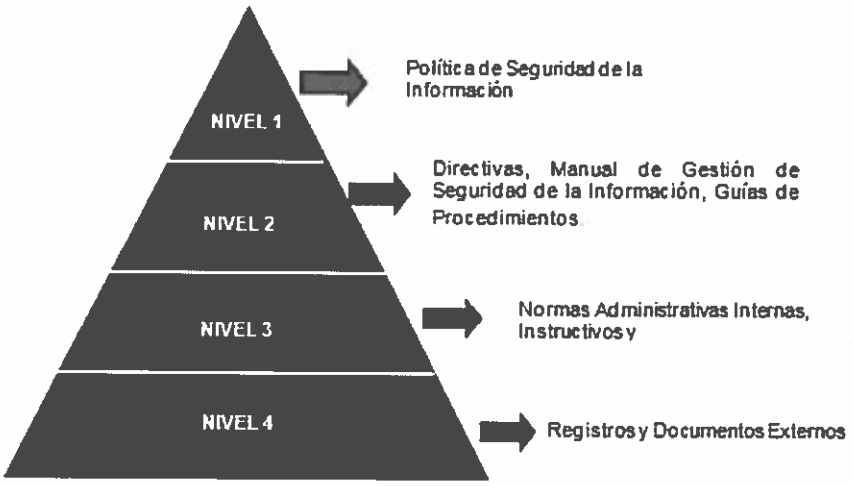

FIGURA N° 06: ESTRUCTURA DE LA DOCUMENTACIÓN DEL SGSI-GCI

7.5.3.2 Manual del Sistema de Gestión de Seguridad de la Información

El Equipo de Gestión de Seguridad de la Información, mantiene actualizado y verifica el cumplimiento del Manual de Gestión de Seguridad de la Información, para dar respuesta a los requisitos de la NTP-ISO/IEC 27001:2014.

Adicionalmente, los documentos normativos del Sistema de Gestión de Seguridad de la Información son registrados por el Gestor Líder de la GCI, en la "Lista maestra de documentos", que se detalla en el Anexo N° 05.

7.5.3.3 Clasificación de la Información

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

7.5.3.4 Disponibilidad de la información

Las versiones vigentes de los documentos normativos se exhiben en la Intranet. Las copias impresas de documentos normativos, se consideran como "Copia no Controlada"

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

- Link en la intranet RENIEC.
- Copia física controlada (En caso se requiera)

A fin de asegurar que los documentos normativos vigentes aplicables a los procesos se encuentren disponibles para el personal que no cuente con equipos informáticos, se identificará un punto de uso. Para ello o cuando se requiera, el Gestor Operativo dispondrá de copias físicas debidamente identificadas con el sello "Copia Controlada", registrándola en la "Lista de distribución de documentos" (Anexo N° 06).

Las versiones vigentes de los documentos normativos se exhiben en la Intranet. Las copias impresas de documentos normativos que no tengan sello "Copia Controlada", se considera "Copia no controlada".

Al aprobarse nuevas versiones de los documentos normativos, se elaboran controles de cambios descriptivos, en los que se detallan y justifican los cambios en los procedimientos.

Cuando se actualiza un documento normativo, las copias controladas de la versión anterior serán recuperadas por los Gestores Operativos de Seguridad de la Información de cada sub proceso, para su eliminación, registrándose en el Anexo N° 07 "Acta de Eliminación".

La Sub Gerencia de Sistematización Jurídica adscrita a la Gerencia de Asesoría Jurídica, a través de la Guía de Procedimientos GP-399-GAJ/SGSJ/004, "Sistematización de documentación y normatividad interna y externa del RENIEC", establece los lineamientos y acciones a seguir para la adecuada sistematización y control de los documentos de origen externo.

El Proceso de "Gestión de Seguridad y Defensa Nacional", mantiene sus registros conforme a la Directiva 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 Líder u Operativo, el responsable de los registros propios del SGSI de su respectivo proceso.

VIII. OPERACIÓN

8.1 Planificación y control operacional

El Sistema de Gestión de Seguridad de la Información del "Proceso Asesoramiento en la Gestión de la Calidad e Innovación", planifica, implementa y controla los procesos necesarios para cumplir con los requisitos de seguridad de la información detallados en el presente manual.

8.2 Evaluación de riesgo de seguridad de la información

En el Sistema de Gestión de Seguridad de la Información del "Proceso Asesoramiento en la Gestión de la Calidad e Innovación" se ejecuta el proceso de gestión riesgos de seguridad de la información a intervalos planificados, según lo dispuesto por la Oficina de Seguridad y Defensa Nacional. La periodicidad será de un año, alineado a cada ciclo del Sistema de Gestión de Seguridad de la Información o cuando se produzcan cambios significativos en la seguridad de la información.

8.3 Tratamiento de riesgo de seguridad de la información

En el Sistema de Gestión de Seguridad de la Información del "Proceso Asesoramiento en la Gestión de la Calidad e Innovación", conforme a lo previsto en la Directiva **DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información"**, se planifican las actividades, responsables, fechas, etc. para tratar los riesgos de nivel importante y crítico, y realizar seguimiento mediante el Plan de Tratamiento de Riesgos y Oportunidades de Seguridad de la Información.

IX. EVALUACIÓN DEL DESEMPEÑO

9.1 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 Sistema de Gestión de Seguridad de la Información, El Gestor Líder y la Oficina de Seguridad y Defensa Nacional establecen 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 de 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 Sistema de Gestión de Seguridad de la Información.

Los indicadores diseñados para el seguimiento del Sistema de Gestión de Seguridad de la Información, así como los resultados alcanzados se enuncian y registran en el **"Sistema de Gestión de Seguridad de la Información - SGSI Cuadro de Mando Operativo – CMO " (Anexo N° 08)**

El resultado de las mediciones, es analizado y evaluado por los Gestores Líderes de Seguridad de la Información, quienes informan al Comité Interno de Seguridad de la Información y a la Oficina de Seguridad y Defensa Nacional, 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 Sistema de Gestión de Seguridad de la Información, 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".**

9.2 Auditoría Interna

La Gerencia de Calidad e Innovación (Dueño del Proceso),en coordinación con la Sub Gerencia de Calidad, planifica y desarrolla las auditorías internas a los sistemas de gestión implementados, de conformidad a los lineamientos establecidos en el documento **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 selección y calificación de auditores.
- 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 Sistema de Gestión de Seguridad de la Información.

9.3 Revisión por la Dirección

La Alta Dirección a través del RAD del RENIEC, realiza revisiones de los Sistemas 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 Gerencia de Calidad e Innovación los criterios para la revisión anual de la dirección del Sistema de Gestión de Seguridad de la Información.

La Revisión por la Dirección-incluye consideraciones de:

a. El estado de las acciones con relación a las anteriores revisiones por 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:

   1. No conformidades y acciones correctivas;
   2. Resultados del monitoreo y medición;
   3. Resultados de auditoria; y
   4. 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 Dirección incluyen decisiones relacionadas a las oportunidades de mejora y cualquier necesidad de cambio, los mismos que son documentados mediante Actas de la revisión de gestión, las que son custodiadas por el Representante de la Alta Dirección. El Sistema de Gestión de Seguridad de la Información del "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación" mantiene información documentada de los resultados de las revisiones de la Alta Dirección.

El Sistema de Gestión de Seguridad de la Información del "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación" mantiene información documentada de los resultados de las revisiones de la Alta Dirección.

El Gestor Líder del "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación realiza el seguimiento de los acuerdos y de las acciones aprobadas y comunica el estado de los mismos al CIGSI y a la Oficina de Seguridad y Defensa Nacional.

X. MEJORAS

10.1 No conformidades y acciones correctivas

La Gerencia Calidad e Innovación (Dueño del Proceso), gestiona los Hallazgos conforme a la Directiva **DI-421-GCI/012 "Tratamiento De Hallazgos"**, en la que se establece lineamientos para identificar, investigar y eliminar las causas de no conformidades reales o potenciales que puedan generarse como resultado de las auditorías internas/externas, resultado de la revisión por la 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.

10.2 Mejora Continua

El "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación", implementa mejoras a sus procesos y controles de seguridad de la información mediante la propuesta de mejoras provenientes de:

- 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.
- Resultados de la medición de indicadores de seguridad de la información.
- Los resultados de las acciones correctivas que incluyen acciones de mejora.

XI. VIGENCIA

Entrará en vigencia a partir de su aprobación.

XII. APROBACIÓN

Será aprobada mediante Resolución Secretarial.

XIII. ANEXOS

ANEXO Nº 01

MATRIZ DE EXPECTATIVAS Y NECESIDADES DE LAS PARTES INTERESADAS

RENIEC

MATRIZ DE EXPECTATIVAS Y NECESIDADES DE LAS PARTES INTERESADAS

PROCESO		RESPONSABLE	

Proceso clave	Unidad orgánica	Proceso	Producto	Grupo de Interés	Expectativas y necesidades	Requisitos

ANEXO Nº 02

FORMATO PARA "LISTA DE CONTACTOS EXTERNOS"

LISTA DE CONTACTOS EXTERNOS

Nº	ORGANIZACIÓN	CONTACTO	CARGO	TELEFONO	CELULAR	E-MAIL

ANEXO N° 03

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

VISIÓN

Formar parte de cada familia y del desarrollo de nuestro país, como la entidad de registros del Estado Peruano que garantiza a las personas su identidad, sus actos de vida y otorga confianza y seguridad jurídica, y provee información electrónica a través de la tecnología de información y comunicaciones.

Sistema de Gestión de Seguridad de la Información

Matriz de planificación de los Objetivos específicos de Seguridad de la Información

	Específico					Medible						Alcanzable		Realista			Límite de tiempo		
Estrategia SMART	Proceso	Objetivo general	Objetivo general de seguridad de la información	Objetivo específico SGSI	Meta	Código indicador	Indicadores		Fuente de los datos	Formula	Frecuencia de medición	Iniciativa estratégica	Responsable	Recursos disponibles			Fecha inicio	Fecha término	Estado
							Nombre	Unidad de medida						Financieros	Humanos	Tiempo			

Oficina de Seguridad y Defensa Nacional - RENIEC

ANEXO N° 04

MATRIZ DE REQUISITOS DE COMPETENCIAS PARA LOS ROLES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) DEL PROCESO DE ASESORAMIENTO EN LA GESTIÓN DE LA CALIDAD E INNOVACIÓN

MATRIZ DE REQUISITOS DE COMPETENCIAS PARA LOS ROLES DEL SGSI - GCI

Aprobado por: GERENCIA DE CALIDAD E INNOVACION	Fecha de aprobación:

No.	Roles	NIVEL EDUCATIVO					GRADO (SITUACIÓN ACADÉMICA Y ESTUDIOS REQUERIDOS PARA EL PUESTO)							Formación con especialidad en alguno de los siguientes rubros o una combinación de estos							Experiencia laboral en años	Competencias	Otras competencias + Habilidades o destrezas
		Primaria	Secundaria Completa	Técnica Básica (1 a 2 Años)	Técnica Superior (3 a 4 Años)	Universitario	Egresado	Bachiller	Titulado/Licenciado	Maestría		Doctorado		Derecho	Economía	Ingeniería	Administración	Computación e Informática	Contabilidad	Otras profesiones	Laboral Total	Tipo / Nivel de Jerarquía
										Egresado	Título	Egresado	Título									
1																						
2																						
3																						
4																						
5																						
6																						
7																						

NOTA: Orientaciones para el uso de la matriz de competencias:

1. **Para campo Educación:**
   a. La educación está referida al tipo de estudios realizados 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 educación marcada"

2. **Para campo Formación:**
   a. La formación está 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 marcadas"

3. **Para campo Experiencia laboral:**
   a. La experiencia está 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 el campo de Competencias:**
   a. Se selecciona de la DI-412-GTH/013 "Gestión del Rendimiento"

COMPETENCIAS (DI-[illegible])			
(CT) - TRANSVERSALES SERVIR CT1 Orientacion a los Resultados CT2 Trabajo en Equipo CT3 Vocacion de Servicio	(CM) - MEJORA DEL SERVICIO CM1 Comunicacion CM2 Capacidad de Analisis CM3 Discrecionalidad y Etica CM4 Liderazgo CM5 Innovacion	(CA) - ATENCION DE SECTORES VULNERABLES CA1 Comunicacion CA2 Capacidad de Analisis CA3 Discrecionalidad y Etica CA4 Liderazgo CA5 Innovacion	(CI) - INNOVACION Y USO INTENSIVO DE LA TECNOLOGIA CI1 -Comunicacion CI2 Capacidad de analisis CI3 Discrecionalidad y Etica CI4 Liderazgo CI5 Innovacion

ANEXO N° 05

LISTA MAESTRA DE DOCUMENTOS

Gerencia de Registros de Identificación

LISTA MAESTRA DE DOCUMENTOS DEL PROCESO DE ASESORAMIENTO EN LA GESTION DE LA CALIDAD E INNOVACION

FECHA:

ITEM	CÓDIGO DEL DOCUMENTO	TIPO DE DOCUMENTO	NOMBRE DEL DOCUMENTO	VERSIÓN	DOCUMENTO QUE APRUEBA	FECHA DE APROBACIÓN	DISPONIBLE EN	APLICACIÓN DE

Firma y sello del Dueño del proceso

ANEXO N° 06

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° 07

ACTA DE ELIMINACIÓN

De acuerdo con lo dispuesto en el Manual de Seguridad de la Información del "Proceso de Asesoramiento en la Gestión de la Calidad e Innovación", vigente, habiéndose aprobado la _____ versión del documento normativo _____,

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 Líder / Operativo de la información
Nombre: DNI N°:	Nombre: DNI N°:

ANEXO N° 08

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

CUADRO DE MANDO OPERATIVO – CMO

Sistema de Gestión de Seguridad de la Información - SGSI
Cuadro de Mando Operativo - CMO

Código de Indicador	Nombre del Indicador	Dimension que miden	Meta	Nivel de Indicador			Promedio Anual		Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	PROMEDIO
				Bueno	Aceptable	Malo	2017								