

DIRECTIVA

**CLASIFICACIÓN DE LA
INFORMACIÓN DEL SISTEMA DE
GESTIÓN DE SEGURIDAD DE LA
INFORMACIÓN**

RESOLUCIÓN SECRETARIAL N° 105 -2019/SGEN/RENIEC		
DI-373-OSDN/007	VERSION: 02	FECHA DE APROBACIÓN <i>02/10/2019</i>
	N° PÁGINAS: 19	

ÍNDICE

- I. OBJETIVO
- II. ALCANCE
- III. BASE LEGAL
- IV. DEFINICIÓN DE TÉRMINOS
- V. RESPONSABILIDAD
- VI. DISPOSICIONES GENERALES
- VII. VIGENCIA
- VIII. APROBACIÓN
- IX. ANEXOS
 - ANEXO N° 01: LISTADO DE CLASIFICACIÓN Y ACCESO A LA INFORMACIÓN
 - ANEXO N° 02: CUADRO DE CONTROL DE CAMBIOS DE LA DI-373-OSDN/007



I. OBJETIVO

Establecer lineamientos a seguir para la clasificación, tratamiento y desclasificación de la información de los Órganos y Unidades Orgánicas del RENIEC en lineamiento con la NTP ISO/IEC 27001:2014 Sistemas de Gestión de Seguridad de la Información (SGSI), normas de transparencia y acceso a la información pública.

II. ALCANCE

La presente Directiva es administrada por la Oficina de Seguridad y Defensa Nacional (OSDN) en coordinación con la Oficina de Administración Documentaria (OAD) y la Oficina de Administración de Archivos (OAA) y es de aplicación obligatoria para todos los Órganos y Unidades Orgánicas en el Registro Nacional de Identificación y Estado Civil en adelante RENIEC.

III. BASE LEGAL

- 3.1 **Ley N° 26497**, Ley Orgánica del Registro Nacional de Identificación y Estado Civil, del 12 julio de 1995 y sus modificatorias.
- 3.2 **Ley N° 25323**, Ley Sistema Nacional de Archivos, del 11 de junio de 1991.
- 3.3 **Ley N° 28716**, Ley de Control Interno de las Entidades del Estado, del 18 de abril de 2006 y sus modificatorias.
- 3.4 **Decreto Supremo N° 004-2019-JUS**, que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, del 25 de enero de 2019.
- 3.5 **Decreto Supremo N° 043-2003-PCM**, que aprueba el Texto Único Ordenado de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública del 24 de abril de 2003 y sus modificatorias.
- 3.6 **Decreto Legislativo N° 1412**, que aprueba la Ley de Gobierno Digital del 13 de setiembre de 2018.
- 3.7 **Decreto Supremo N° 008-92-JUS**, Reglamento de la Ley N° 25323 que crea el Sistema Nacional de Archivos, del 27 de junio de 1992 y sus modificatorias.
- 3.8 **Decreto Supremo N° 019-2017-JUS**, Reglamento del Decreto Legislativo N° 1353, Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses, del 15 setiembre de 2017 y sus modificatorias.
- 3.9 **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.
- 3.10 **Resolución Ministerial N° 166-2017-PCM**, modifica el Art. 5 de la R. M. N° 004-2016-PCM, referente al Comité de Gestión de Seguridad de la Información, del 21 de junio de 2017.
- 3.11 **Resolución Ministerial N° 087-2019-PCM**, aprueban disposiciones sobre la conformación y funciones del Comité de Gobierno Digital, del 22 de marzo de 2019.
- 3.12 **Resolución de Contraloría N° 320-2006-CG**, que aprueban las Normas de Control Interno, del 03 de noviembre de 2006.



- 3.13 **Resolución de Contraloría N° 146-2019-CG**, que aprueba la Directiva N°006-2019-CG/INTEG "Implementación del Sistema de Control Interno de las Entidades del Estado", del 17 de mayo de 2019.
- 3.14 **Resolución Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias N° 129-2014/CNB-INDECOPI**, que aprueban Normas Técnicas Peruanas sobre la tecnología de la información, alimentos obtenidos por medios biotecnológicos modernos y otros, del 01 de diciembre de 2014.
- 3.15 **Resolución Jefatural N° 028-2019-AGN/J**, que aprueba la Directiva DI-008-2019-AGN/DDPA, "Directiva para la elaboración del programa de control de documentos de las Entidades Públicas", del 28 de enero de 2019.
- 3.16 **Resolución Jefatural N° 000073-2016/JNAC/RENIEC**, aprueba el Reglamento de Organización y Funciones y la Estructura Orgánica del RENIEC, del 01 de junio de 2016.
- 3.17 **Resolución Jefatural N° 000021-2019/JNAC/RENIEC, inciso i)** delega a la Secretaría General la facultad de "Disponer mediante la emisión del acto administrativo correspondiente la recuperación o reconstrucción de la información afectada por extravío, destrucción, extracción, alteración, o modificación indebida de información en poder de la Entidad, a efectos de su recuperación o reconstrucción", del 11 de febrero de 2019.
- 3.18 **Resolución Jefatural N° 028-2019 AGN/J**, que aprueba la Directiva N° 0008-2019-AGN/DDPA Directiva para la elaboración del programa del control de documentos de las entidades públicas, del 28 de enero de 2019.
- 3.19 **Resolución Jefatural N° 000073-2015/JNAC/RENIEC**, que aprueba la Política de Seguridad de la Información del RENIEC, del 30 de marzo de 2015.
- 3.20 **Resolución Jefatural N° 000071-2018/JNAC/RENIEC**, que actualiza el programa de control de documentos del RENIEC, del 19 de junio de 2018.
- 3.21 **Resolución Jefatural N° 000096-2018/JNAC/RENIEC**, que designa al abogado Juan Manuel Merino Medina, Jefe encargado de la Oficina de Administración de Archivos de la Secretaria General, como funcionario responsable de la clasificación, reclasificación y desclasificación de la información, según corresponda, de la información secreta reservada y confidencial del Registro Nacional de Identificación y Estado Civil, RENIEC, del 28 de agosto de 2018.
- 3.22 **Resolución Secretarial N° 000063-2017/SGEN/RENIEC**, que aprueba la Directiva DI-417-SGEN/010 "Gestión Documental del RENIEC", del 15 de setiembre de 2017.
- 3.23 **Resolución Secretarial N° 000055-2017/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 y su modificatoria.
- 3.24 **Resolución Secretarial N° 000037-2019/SGEN/RENIEC**, que aprueba la Directiva DI-422-SGEN/OAA/007 "Reconstrucción de Documentos del RENIEC" primera versión, del 12 de abril de 2019.
- 3.25 **Resolución Secretarial N° 000004-2015/SGEN/RENIEC**, que aprueba la Directiva DI-366-GCI/007 "Gestión por Procesos del RENIEC", primera versión, del 27 de enero de 2015.



- 3.26 **Resolución Gerencial N° 00004-2016/GCI/RENIEC**, que aprueba la Directiva DI-372-OSDN/006 "Gestión de Riesgos de Seguridad de la Información", segunda versión, del 21 de noviembre de 2016.

IV. DEFINICIÓN DE TÉRMINOS

4.1 Activo de Información

Es cualquier dato o información que se relaciona con la captura, tratamiento, almacenamiento y presentación de la misma, los cuales tienen un valor para la organización.

4.2 Clasificación

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

4.3 Custodio de la información

Área o responsable del RENIEC que en el marco de sus funciones vigila o resguarda la información considerando las normas y disposiciones aplicables.

4.4 Desclasificación

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

4.5 Documento de archivo

Información producida (recibido o emitido) en el ejercicio de una función, procedimiento, actividad, tarea o acción por la entidad de cualquier fecha, forma, soporte físico y cualquier otro que se genere como resultado del avance tecnológico. Por ejemplo: Carta, Dictamen Legal, Hoja de Elevación, Hoja de Envío, Hoja de Estudio y Opinión, Informe, Informe Técnico de Bienes Patrimoniales, Memorando, Memorando Múltiple, Oficio, Oficio Circular, Proveído, Resolución, Síntesis Ejecutiva y Solicitud Interna, entre otros.

4.6 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 de extremo a extremo (gestión de principio a fin del proceso transversal).

4.7 Etiquetado

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

4.8 Gestor Líder de Seguridad de la Información

Rol asumido por un servidor civil designado por el dueño del proceso, que lidera la implementación y el mantenimiento del SGSI en el ámbito de su competencia.

4.9 Gestor Operativo de Seguridad de la Información

Rol asumido por un servidor civil designado por el dueño del proceso, que apoya la implementación y el mantenimiento del SGSI en el ámbito de su competencia.



4.10 Información

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

4.11 Programa de Control de Documentos

Documento de gestión archivística que establece las series documentales que produce la entidad como resultado de sus actividades, precisando el número de años que debe conservarse y los periodos o plazos de retención de cada documento hasta su transferencia al archivo central o su eliminación.

4.12 Medio de soporte

Es aquel que se utiliza para el almacenamiento y procesamiento de datos, ya sea en forma física o digital.

4.13 Propietario de la información

Máxima autoridad de RENIEC responsable de clasificar dicha información o en todo caso designar a los funcionarios encargados de realizarla.

4.14 Riesgo

Es la posibilidad de ocurrencia de un evento adverso o positivo, que afecte o genere una oportunidad, respecto al cumplimiento de los objetivos institucionales (en los niveles: operacional, táctico y estratégico).

4.15 Serie Documental

Conjunto de documentos (expedientes) que tiene características comunes, el mismo tipo documental o el mismo asunto y que, por consiguiente, son archivados, usados, transferidos y pueden ser eliminados como unidad.

4.16 Sistema de Gestión de Seguridad de la Información

Es un enfoque sistémico que consiste en políticas, procedimientos, directrices, asociada a recursos y actividades colectivamente gestionadas por una organización, en la búsqueda de la protección de sus activos de información mediante el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora de la seguridad de la información de una organización para alcanzar sus objetivos.

V. RESPONSABILIDAD

5.1 La OSDN a través de la Sub Gerencia de Seguridad de la Información (OSDN/SGSI) en coordinación con la OAA de la Secretaria General (SGEN), debe realizar las siguientes actividades:

- 5.1.1 Brindar asesoramiento en la implementación y ejecución de la clasificación de la información.
- 5.1.2 Establecer los niveles de clasificación de la información.
- 5.1.3 Determinar el tratamiento de la información clasificada.



5.2 Es responsabilidad del Dueño del Proceso coordinar la revisión, proponer la clasificación al Propietario de la Información, tratar la información e implementar controles de seguridad de la información según los lineamientos de la presente Directiva, en el ámbito de su competencia.

5.3 Es responsabilidad de la OAA de la SGEN, en calidad de Propietario de la Información designado por la JNAC, lo siguiente:

5.3.1 Ejecutar acciones orientadas a salvaguardar la integridad física del Fondo Documental, incluidas las microformas del RENIEC.

5.3.2 Clasificar y desclasificar, según corresponda, de la información secreta, reservada y confidencial del RENIEC, a que se refiere el Texto Único Ordenado por Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, su Reglamento y modificatoria, aprobados por los Decretos Supremos N° 043-2013-PCM, 072-2003-PCM y 070-2013-PCM.

5.3.3 Ejecutar las acciones orientadas al cumplimiento de los procesos técnicos archivísticos (organización, custodia, transferencia y eliminación) y a la custodia del patrimonio documental del RENIEC, en concordancia de los lineamientos del Archivo General de la Nación.

5.3.4 Proponer las medidas de seguridad de la documentación que se custodia en el sistema de archivo institucional, que permita la defensa, conservación e incremento del patrimonio documental de la institución en coordinación con la OSDN.

5.4 Es responsabilidad de la OAD de la SGEN, lo siguiente:

5.4.1 Gestionar acciones relativas al procedimiento de atención de las solicitudes de información en el marco de la Ley de Transparencia y Acceso a la Información Pública en el ámbito de su competencia.

5.4.2 Atender las solicitudes y proporcionar la información requerida en aplicación de la Ley de Transparencia y Acceso a la Información Pública en el ámbito de su competencia.

5.5 Es responsabilidad del Gestor Líder de Seguridad de la Información coordinar las acciones para la clasificación de la información, etiquetado y uso adecuado de los activos de seguridad de la información con la OSDN/SGSI, OAA y OAD.

5.6 Es responsabilidad del Gestor Operativo de Seguridad de la Información:

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

5.6.2 Realizar el etiquetado o marcado de la información, donde corresponda.

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

5.7 Es responsabilidad del Oficial de Seguridad de la Información, coordinar con la OSDN/SGSI, Gestores Líderes y Operativos de Seguridad de la Información, Órganos y Unidades Orgánicas competentes del RENIEC la implementación y el cumplimiento de la presente Directiva en el marco del SGSI.



VI. DISPOSICIONES GENERALES

6.1 La clasificación de la información comprende las siguientes actividades:

- 6.1.1 Establecer los niveles de clasificación a la información.
- 6.1.2 Aprobar la clasificación de la información.
- 6.1.3 Etiquetar la información.
- 6.1.4 Realizar el tratamiento de la información.
- 6.1.5 Desclasificar la información.

6.2 La OAD establecerá los lineamientos a seguir para la atención de solicitudes de acceso a la información pública en cumplimiento de la Ley N° 27806 "Ley de Transparencia y Acceso a la Información Pública" y su reglamento.

VII. DISPOSICIONES ESPECÍFICAS

7.1 ESTABLECIMIENTO DE LOS NIVELES DE LA INFORMACIÓN CLASIFICADA

7.1.1 Para realizar la clasificación de la información se debe considerar como insumo lo siguiente:

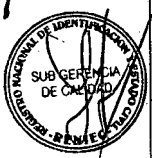
- Inventario de activos de información, definido en la DI-372-OSDN/006, en aquellos procesos que cuentan o están en proceso de implementación de un SGSI.
- Programa de Control de Documentos de acuerdo a los lineamientos establecidos por la OAA.

7.1.2 La clasificación de la información se realizará utilizando el formato: "Listado de Clasificación y acceso a la Información" (ver Anexo N° 01) según los niveles de clasificación definidos en el siguiente cuadro:

CLASIFICACIÓN DE LA INFORMACIÓN		
NIVEL	DESCRIPCIÓN	REQUISITO LEGAL
PÚBLICA	<ul style="list-style-type: none"> • Todo documento en cualquier formato que se encuentre en poder de las Instituciones Públicas. • Toda información que puede ser conocida por el público en general. • Su difusión no representa riesgo alguno para la continuidad de las operaciones del RENIEC. 	<ul style="list-style-type: none"> - Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública y su modificatoria.
CONFIDENCIAL	<ul style="list-style-type: none"> • Consejos, recomendaciones u opiniones previas a la toma de una decisión del RENIEC, salvo que sea pública. • Información bancaria, tributaria, comercial, industrial, tecnológica y 	<ul style="list-style-type: none"> - Ley 27806, Ley de Transparencia y Acceso a la Información Pública y su modificatoria.



CLASIFICACIÓN DE LA INFORMACIÓN		
NIVEL	DESCRIPCIÓN	REQUISITO LEGAL
	<p>bursátil regulada por la legislación pertinente.</p> <ul style="list-style-type: none"> Datos personales (invade la intimidad personal o familiar). Información vinculada a investigaciones en trámite referidas al ejercicio de la potestad sancionadora de la Administración Pública. Información preparada u obtenida por asesores jurídicos o abogados que pudieran revelar la estrategia en la tramitación o defensa en un proceso administrativo o judicial. <p>Su difusión o uso no autorizado puede representar riesgos al proceso y/o incumplimiento de las normas legales.</p>	<ul style="list-style-type: none"> Ley 29733, Ley de Protección de Datos Personales. Ley 27444, Ley de Procedimiento Administrativo y su modificatoria.
RESERVADA	<p>Se considera aquella información que por razones de seguridad nacional en el ámbito del orden interno originaría un riesgo a la integridad territorial y/o estabilidad democrática, así mismo en el ámbito del orden externo originaría un riesgo en las negociaciones internacionales y/o subsistencia del sistema democrático.</p> <p>Su difusión o uso no autorizado representa un alto riesgo a la confidencialidad, disponibilidad e integridad del proceso.</p>	Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública y su modificatoria.
SECRETA	<p>Se considera aquella información relacionada al ámbito militar, de inteligencia y contrainteligencia.</p> <p>Su revelación originaría riesgos a la: Seguridad Nacional (vida e integridad de las personas que desarrollan actividades en dicho ámbito), integridad territorial y subsistencia del sistema democrático.</p>	Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública y su modificatoria.



7.2 APROBACIÓN DE LA INFORMACIÓN CLASIFICADA

- 7.2.1 Los Órganos y Unidades Orgánicas de la Entidad deberán enviar a la OAA el "Listado de Clasificación y acceso a la Información" con copia a la OSDN, a fin de proceder con la aprobación de la Clasificación a la Información.
- 7.2.2 La OAA solicitará subsanar observaciones en el "Listado de Clasificación y acceso a la Información" a los Órganos y Unidades Orgánicas de ser el caso.
- 7.2.3 La OAA aprobará la clasificación a la información, mediante resolución gerencial.

7.3 ETIQUETADO A LA INFORMACIÓN CLASIFICADA

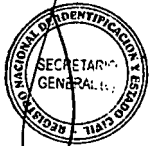
- 7.3.1 Los medios de soporte y/o unidad de archivamiento que contengan información clasificada deberán ser identificados mediante etiquetas o rótulos, cuando corresponda.
- 7.3.2 En los casos en que el medio de soporte contenga información con distintos niveles de clasificación, el etiquetado será en función al de mayor nivel de clasificación.
- 7.3.3 En el siguiente cuadro se especifica los criterios de etiquetado:

CRITERIOS DE ETIQUETADO	
NIVEL	ETIQUETADO
PÚBLICA	No requiere etiquetado.
CONFIDENCIAL	Si requiere etiquetado.
RESERVADA	Si requiere etiquetado.
SECRETA	Si requiere etiquetado.

7.4 TRATAMIENTO DE LA INFORMACIÓN CLASIFICADA

- 7.4.1 La información deberá ser protegida de acuerdo al nivel de clasificación asignada, conforme a lo indicado en el siguiente cuadro:

TRATAMIENTO DE LA INFORMACIÓN CLASIFICADA	
NIVEL	DESCRIPCION
PÚBLICA	<ul style="list-style-type: none"> - ALMACENAMIENTO: Su almacenamiento se debe efectuar de acuerdo a la normativa vigente establecida para tal fin. - RESPALDO: Se debe efectuar de acuerdo a las consideraciones del Dueño del Proceso en



TRATAMIENTO DE LA INFORMACIÓN CLASIFICADA	
NIVEL	DESCRIPCION
	<p>coordinación con el Propietario de la Información dada la criticidad de la información.</p> <ul style="list-style-type: none"> - ACCESO: Se efectúa respetando la Ley de Transparencia y Acceso a la Información Pública, así como otras normativas a través de los canales autorizados por el RENIEC. - OTRAS MEDIDAS DE CONTROL: Se efectúa considerando la evaluación de riesgos de seguridad de la información con los órganos involucrados.
<p>CONFIDENCIAL RESERVADA SECRETA</p>	<ul style="list-style-type: none"> - ALMACENAMIENTO: Su almacenamiento se debe efectuar de forma segura, protegida y con sistema de acceso controlado. - RESPALDO: Se debe efectuar de acuerdo a las consideraciones Dueño del Proceso en coordinación con el Propietario de la Información dada la criticidad de la información. - ACCESO: Se efectúa respetando la Ley de Transparencia y Acceso a la Información Pública, así como otras normativas a través de los canales autorizados por el RENIEC. - OTRAS MEDIDAS DE CONTROL: Se efectúa considerando la evaluación de riesgos de seguridad de la información con los órganos involucrados.

7.5 DESCLASIFICACIÓN DE LA INFORMACIÓN

7.5.1 El proceso de desclasificación de la información, se llevará a cabo a solicitud del Propietario de la Información en coordinación con el Dueño del Proceso.

7.5.2 El "Listado de Clasificación y Acceso a la Información" (Anexo 01) deberá actualizarse como mínimo anualmente, siendo responsabilidad del Dueño del Proceso informar a la OSDN (a través de la OSDN/SGSI) y OAA del estado del mismo.

VIII. DISPOSICIÓN COMPLEMENTARIA

Cualquier situación no contemplada en la presente directiva respecto a la clasificación de la información del RENIEC, deberá ser informada a la SGEN y la OSDN para su gestión.

IX. VIGENCIA

Entrará en vigencia a partir de su aprobación



X. APROBACIÓN

Será aprobada mediante Resolución Secretarial.

XI. ANEXOS





CLASIFICACIÓN DE LA INFORMACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

DI-373-OSDN/007



- (1) Nombre del proceso según ingeniería de proceso.
- (2) Fecha de actualización del documento.
- (3) Versión del documento en el ciclo de implementación o mantenimiento (1, 2, 3, etc.).
- (4) Código del activo de información según lo establecido por OSDN.
- (5) Código de la serie documental, en caso aplique.
- (6) Nombre del órgano y/o unidad orgánica de la información clasificada.
- (7) Nombre del activo de información según el Formato de Inventario de Activos de Información.
- (8) El "MEDIO DE SOPORTE" puede ser una categoría o ambas:

- Físico
- Digital



- (9) Descripción de la información clasificada.
- (10) Documentos que sustentan la serie documental o información clasificada.
- (11) La forma en la que se puede tener acceso a la información de manera interna.
- (12) La forma en la que se puede tener acceso a la información de manera externa.
- (13) La "CLASIFICACIÓN" puede ser la siguiente:

- Pública
- Confidencial
- Reservada
- Secreta



- (14) El alcance de la clasificación que tiene la información o si agrupa otras clasificaciones.
- (15) Persona, gerencia o unidad orgánica que verifica el cumplimiento normativo con respecto a las reglas de uso.
- (16) Persona, gerencia o unidad orgánica que tiene acceso a la información cumpliendo con la normatividad de las reglas de uso asociadas.
- (17) Los tipos pueden ser los siguientes:





- Permanente
- Temporal

(18) Tiempo en el cual la información está a cargo de la gerencia o unidad orgánica.

(19) Comentario adicional con respecto a la información clasificada.

(20) Lo elabora el Gestor Líder u Operativo.

(21) Lo revisa el Sub Gerente o Gerente.

(22) Lo aprueba el responsable de la OAA de la SGEN.

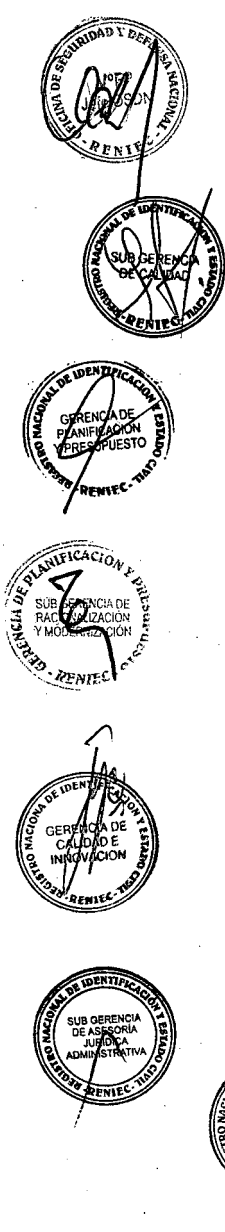


Anexo N° 02

Cuadro de Control de Cambios de la DI-373-OSDN/008

CUADRO DE CONTROL DE CAMBIOS DE LA DI-373-OSDN/008 "CLASIFICACIÓN DE LA INFORMACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN"	
IDENTIFICACIÓN DEL CAMBIO	
Numeral vigente	Numeral modificado
I.OBJETIVO	I.OBJETIVO
II. ALCANCE	II. ALCANCE
III. BASE LEGAL	III. BASE LEGAL
No existía en esta versión	Numeral 3.2
Numeral 3.2	Numeral 3.3
Numeral 3.3	Numeral 3.5
Numeral 3.4	Numeral 3.5
Numeral 3.5	Se eliminó
No existía en esta versión	Numeral 3.6
No existía en esta versión	Numeral 3.7
No existía en esta versión	Numeral 3.8
No existía en esta versión	Numeral 3.9
No existía en esta versión	Numeral 3.10
No existía en esta versión	Numeral 3.11
Numeral 3.6	Numeral 3.12
Numeral 3.7	Se eliminó
Numeral 3.8	Se eliminó
Numeral 3.9	Se eliminó
Numeral 3.10	Se eliminó
Numeral 3.11	Se eliminó
Numeral 3.12	Se eliminó

SEGUNDA VERSIÓN
RESOLUCION SECRETARIAL N° -2018/SGEN/RENIEC



Numeral 3.13	Se eliminó
No existía en esta versión	Numeral 3.13
No existía en esta versión	Numeral 3.14
No existía en esta versión	Numeral 3.15
No existía en esta versión	Numeral 3.16
No existía en esta versión	Numeral 3.17
No existía en esta versión	Numeral 3.18
No existía en esta versión	Numeral 3.19
No existía en esta versión	Numeral 3.20
No existía en esta versión	Numeral 3.21
IV. DEFINICIÓN DE TÉRMINOS	IV. DEFINICIÓN DE TÉRMINOS
Numeral 4.1	Se modificó
Numeral 4.2	Se eliminó
Numeral 4.3	Se eliminó
No existía en esta versión	Numeral 4.3
No existía en esta versión	Numeral 4.4
No existía en esta versión	Numeral 4.5
No existía en esta versión	Numeral 4.6
Numeral 4.4	Numeral 4.7
No existía en esta versión	Numeral 4.8
No existía en esta versión	Numeral 4.9
Numeral 4.5	Numeral 4.10
No existía en esta versión	Numeral 4.11
Numeral 4.6	Numeral 4.12
Numeral 4.8	Numeral 4.13
No existía en esta versión	Numeral 4.14
No existía en esta versión	Numeral 4.15



Numeral 4.9	Numeral 4.16
V. RESPONSABILIDAD	V. RESPONSABILIDAD
Numeral 5.1	Numeral 5:1
Numeral 5.1.4	Se eliminó
Numeral 5.2	Numeral 5.2
Numeral 5.3	Numeral 5.3
No existía en esta versión	Numeral 5.3.1
No existía en esta versión	Numeral 5.3.2
No existía en esta versión	Numeral 5.3.3
No existía en esta versión	Numeral 5.3.4
Numeral 5.4	Numeral 5.4
Numeral 5.4.1	Numeral 5.4.1
Numeral 5.4.2	Numeral 5.4.2
No existía en esta versión	Numeral 5.5
No existía en esta versión	Numeral 5.6
No existía en esta versión	Numeral 5.6.1
No existía en esta versión	Numeral 5.6.2
No existía en esta versión	Numeral 5.6.3
No existía en esta versión	Numeral 5.7
VI. DISPOSICIONES GENERALES	VI. DISPOSICIONES GENERALES
Numeral 6.1	Numeral 6.1
Numeral 6.1.1	Numeral 6.1.1
Numeral 6.1.2	Numeral 6.1.2
Numeral 6.1.3	Numeral 6.1.3
No existía en esta versión	Numeral 6.1.4
No existía en esta versión	Numeral 6.1.5
Numeral 6.2	Numeral 6.2



Numeral 6.2.1	Se eliminó
Numeral 6.2.2	Se eliminó
Numeral 6.2.3	Se eliminó
Numeral 6.3	Se eliminó
Numeral 6.4	Se eliminó
Numeral 6.4.1	Se eliminó
Numeral 6.4.2	Se eliminó
VII. DISPOSICIONES ESPECÍFICAS	VII. DISPOSICIONES ESPECÍFICAS
No existía en esta versión	Numeral 7.1
No existía en esta versión	Numeral 7.1.1
No existía en esta versión	Numeral 7.1.2
No existía en esta versión	Numeral 7.2
No existía en esta versión	Numeral 7.2.1
No existía en esta versión	Numeral 7.2.2
No existía en esta versión	Numeral 7.2.3
No existía en esta versión	Numeral 7.3
No existía en esta versión	Numeral 7.3.1
No existía en esta versión	Numeral 7.3.2
No existía en esta versión	Numeral 7.3.3
No existía en esta versión	Numeral 7.4
No existía en esta versión	Numeral 7.4.1
No existía en esta versión	Numeral 7.5
No existía en esta versión	Numeral 7.5.1
No existía en esta versión	Numeral 7.5.2
VIII. DISPOSICIÓN COMPLEMENTARIA	VIII. DISPOSICIÓN COMPLEMENTARIA
IX. VIGENCIA	IX. VIGENCIA

