



Política de Seguridad

Servicios de Certificación Digital y Prestación de Servicios de Valor Añadido

Código: DA-DCSD/SDSCD-005

Versión: 8.0

Año: 2024

Elaborado por:

Oficial de Seguridad de la Información - DCSD

Revisado por:

Subdirector de Servicios de Certificación Digital

Aprobado por:

Director de Certificación y Servicios Digitales

Historial de Cambios				
Ver.	Fecha	Descripción	Responsable	Estado
1.0	13/07/2012	Elaboración y aprobación.	GCRD	Aprobado
2.0	20/11/2012	Se recoge observaciones del evaluador de INDECOPI.	GCRD	Aprobado
3.0	05/07/2013	Actualización	GCRD	Aprobado
4.0	15/08/2014	Actualización	GCRD	Aprobado
5.0	10/07/2017	Actualización	GRCD	Aprobado
6.0	02/10/2018	Actualización	GRCD	Aprobado
7.0	01/12/2021	Actualización	DSCD	Aprobado
8.0	03/05/2024	Actualización	DCSD	Aprobado

INDICE

1.	Objetivo	4
2.	Administración del documento	4
3.	Base legal	4
4.	Alcance	5
5.	Responsables	6
6.	Glosario de términos	6
7.	Políticas	8
8.	Referencias	17

1. Objetivo

Establecer el marco general y los lineamientos para la seguridad de la información proveniente del proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido, a fin de garantizar la disponibilidad, confidencialidad e integridad de la información durante el desarrollo de las operaciones y acciones que se realizan.

2. Administración del documento

a) Organización que administra el documento

Registro Nacional de Identificación y Estado Civil – RENIEC.

Dirección: Jr. Bolivia 109, Centro Cívico – Lima, Perú.

Teléfonos: (01) 315 2700 – (01) 315 4000.

b) Persona de contacto

Oficial de Seguridad de la Información de la Dirección de Certificación y Servicios Digitales. Teléfono: (01) 315 2700 – (01) 315 4000 anexo 3016.
Correo electrónico: jmartinezpa@reniec.gob.pe.

3. Base legal

- Ley N° 27269 Ley de Firmas y Certificados Digitales.
- Ley N° 27310 Ley que modifica el artículo 11° de la Ley N° 27269.
- Ley N° 29733 Ley de Protección de Datos Personales.
- Decreto Supremo N° 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales y sus modificatorias.
- Decreto Supremo N° 0003-2013-JUS, Reglamento de la Ley de Protección de Datos Personales.
- Resolución Ministerial N° 129-2012-PCM, del 23 de mayo de 2012, que Aprueba el uso obligatorio de la Norma Técnica Peruana “NTP-ISO/IEC 27001:2008 EDI. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos”.
- Decreto Supremo N°029-2021-PCM, del 19 de febrero de 2021, que aprueba el Reglamento del Decreto Legislativo N°1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
- Decreto Supremo N°157-2021-PCM, Reglamento del Decreto de Urgencia N°006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Resolución de la Comisión para la Gestión de la Infraestructura Oficial de Firma Electrónica N° 075-2019/CFE-INDECOPI, del 2 de mayo de 2019, que aprueba la Guía de Acreditación de Entidad de Certificación, versión 4.1.

- Resolución de la Comisión para la Gestión de la Infraestructura Oficial de Firma Electrónica N° 154-2018/CFE-INDECOPI, del 4 de octubre de 2018, que aprueba la Guía de Acreditación de Entidad de Registro, versión 4.0.
- Resolución Jefatural N° 0162-2022/JNAC/RENIEC, del 26 de setiembre de 2022, que aprueba la Política y Objetivos de la Gestión Integral del Riesgo del RENIEC
- Resolución Secretarial Nro. 0004-2023/SGEN/RENIEC del 09 de enero de 2023, que aprueba la directiva DI-010/OIR/002, “Gestión Integral del Riesgo” primera versión.
- Resolución Jefatural N° 153-2023/JNAC/RENIEC, del 18 de setiembre de 2023, que aprueba la “Política y los Objetivos de Seguridad de la Información” del RENIEC.

4. Alcance

a) Áreas de alcance

El contenido de la presente política, así como las reglas o normas y procedimientos que se deriven de ella, serán de cumplimiento obligatorio por los proveedores, terceros y por todo el personal involucrado en la ejecución directa o indirecta de las actividades que sean parte del proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido.

b) Servicios de alcance

La presente Política de Seguridad de la Información aplica para los siguientes servicios:

Servicio	Descripción del servicio	Unidad responsable
ECEP - RENIEC	Emisión y cancelación de certificados digitales, administración de su ciclo de vida, administración de repositorio y consulta de estado de certificados digitales.	Subdirección de Servicios de Certificación Digital (SDSCD)
EREP - RENIEC	Emisión, cancelación y entrega de certificados digitales, así como la protección de los documentos sustentatorios y su archivo ya sean en formato físico o digital.	Subdirección de Servicios de Certificación Digital (SDSCD) Dirección de Servicios Registrales (DSR)
PSVA - TSA	Emisión de sellado de tiempo que permite atestar que un documento electrónico o cualquier objeto digital existió en un determinado momento en el tiempo y que desde ese momento no fue alterado.	Subdirección de Servicios de Certificación Digital (SDSCD)
Otros servicios	Servicios relacionados con Certificación Digital.	La unidad orgánica que corresponda.

c) **Inclusiones de este documento**

El presente documento incluye los siguientes aspectos: la gestión de riesgos, control de acceso, seguridad de personal, seguridad física, seguridad de comunicaciones y redes, mantenimiento de equipos y su desecho, control de cambios y configuración, planificación de contingencias, respuesta a incidentes, auditorías y detección de intrusiones, medios de almacenamiento y la administración de claves; todos ellos dentro del ámbito de las actividades del proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido.

5. Responsables

- **Responsable de aprobar y apoyar la implementación de la Política de Seguridad de la Información**
 - La Dirección de Certificación y Servicios Digitales - DCSD.
- **Responsable de elaborar, efectuar revisiones periódicas, proponer y apoyar la implementación de la Política de Seguridad de la Información**
 - El Oficial de Seguridad de la Información de la DCSD.
- **Responsables de implementar la Política de Seguridad de la Información**
 - Los órganos del RENIEC involucrados en el proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido; en los aspectos que les correspondan.
- **Responsables de supervisar el cumplimiento de la Política de Seguridad de la Información**
 - El Oficial de Seguridad de la Información de la DCSD.
 - Cada director y subdirector de los órganos del RENIEC involucrados en el proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido.
 - Los supervisores de seguridad de la información y privacidad de datos.

6. Glosario de términos y siglas

- **Activo:** Cualquier cosa que tenga valor para la organización.
- **Análisis de riesgos:** Utilización sistemática de la información disponible para identificar los peligros y para estimar el riesgo.

- **Amenaza:** Causa potencial de un incidente, que puede resultar en un daño hacia individuos, activos, un sistema, una organización, o al ambiente.
- **Control:** Herramienta de la gestión de riesgos, incluido políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal, para prevenir o eliminar un peligro o reducirlo a un nivel aceptable.
- **DCSD:** Dirección de Certificación y Servicios Digitales.
- **DSR:** Dirección de Servicios Registrales.
- **ECEP:** Entidad de Certificación para el Estado Peruano. Cumple con las funciones y obligaciones de una Entidad de Certificación (EC) según lo indicado en el Reglamento de la Ley de Firmas y Certificados Digitales.
- **ECERNEP:** Entidad de Certificación Nacional para el Estado Peruano. Se encarga de emitir los certificados para las Entidades de Certificación para el Estado Peruano intermedias.
- **EREP:** Entidad de Registro o Verificación para el Estado Peruano. Cumple con las funciones y obligaciones de una Entidad de Registro o Verificación (ER) según lo indicado en el Reglamento de la Ley de Firmas y Certificados Digitales.
- **Evaluación del riesgo:** Proceso general que comprende un análisis del riesgo y una valoración del riesgo.
- **Evento de seguridad de la información:** Ocurrencia que indica una posible brecha de seguridad de la información o falla de los controles.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.
- **Identidad digital:** La identidad digital es aquel conjunto de atributos que individualiza y permite identificar a una persona en entornos digitales.
- **Incidente de seguridad de la información:** Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar a los activos de una organización o comprometer sus operaciones.
- **OAF:** Oficina de Administración y Finanzas.
- **OPH:** Oficina de Potencial Humano.
- **OTI:** Oficina de Tecnologías de la Información.
- **PSVA:** Prestador de Servicios de Valor Añadido.
- **Riesgo:** Efecto de la incertidumbre sobre la consecución de los objetivos.
- **SDSCD:** Sub Dirección de Servicios de Certificación Digital.
- **Seguridad de la Información:** Preservación de la confidencialidad, disponibilidad e integridad de la información; asimismo, otras propiedades como la autenticidad, no rechazo, veracidad o confiabilidad.
- **Tratamiento del riesgo:** Proceso de selección e implementación de medidas o controles para modificar el riesgo.
- **TSA:** Autoridad de Sellado de Tiempo.
- **Vulnerabilidades:** Debilidad del activo o control que puede ser aprovechado por una amenaza.

7. Políticas

Genérica

El Registro Nacional de Identificación y Estado Civil reconoce como activo principal la información utilizada y resultante del proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido, y que permite la generación de la identidad digital. En tal sentido, se efectúa la gestión de los riesgos, la aplicación de controles y la concientización en el personal, de modo que nos permita mantener la confidencialidad, integridad y disponibilidad de la misma, así como dar cumplimiento a los requisitos técnicos y legales vigentes.

Específicas

a. Organización

Se ha establecido la siguiente estructura de gestión de la seguridad de la información en el ámbito del proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido, con la finalidad de implementar controles que permitan asegurar la confidencialidad, integridad y disponibilidad de la información.

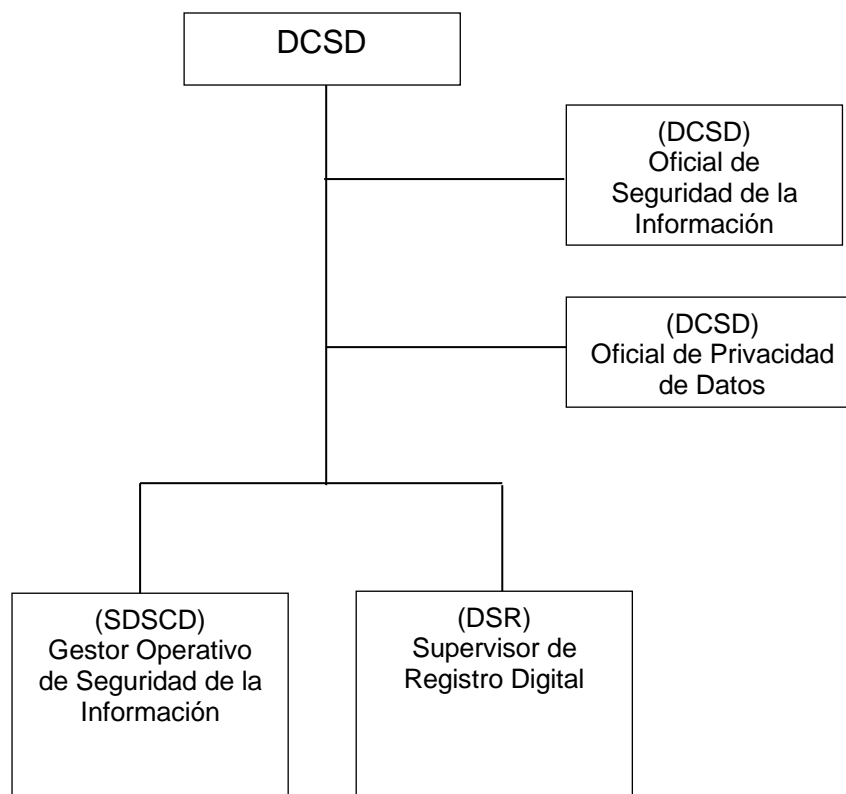


Fig. 1: Estructura de gestión de la Seguridad de la Información.

El Oficial de Seguridad de la Información de la DCSD, tiene entre sus responsabilidades difundir la Política de Seguridad de la Información, así mismo, después de la aprobación de esta política por la DCSD, esta será publicada en la página web institucional para conocimiento de todo el personal de los distintos órganos que intervienen en el proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido, así como de los terceros interesados.

Con la finalidad de garantizar la disponibilidad, confidencialidad e integridad de la información, se deberá realizar revisiones y actualizaciones periódicas de la Política de Seguridad de la Información en concordancia con los riesgos identificados, requerimientos de la entidad, leyes y regulaciones vigentes.

Para asegurar la Protección de Datos Personales se cuenta con un Oficial de Privacidad de Datos de la DCSD, quien es responsable de la supervisión del cumplimiento de la normativa sobre protección de datos personales y la implementación de las acciones respectivas.

Para la supervisión de la Seguridad de la Información se cuenta con un Oficial de Seguridad de Información de la DCSD, quien es responsable de supervisar la implementación de la seguridad de la información, así como de las estrategias, programas, políticas, procedimientos y controles relacionados a la seguridad de la información.

Corresponde al gestor operativo de seguridad de la información y al supervisor de registro digital de las oficinas EREP a cargo de la DSR, verificar el cumplimiento de la Política de Seguridad de la Información y el Plan de Seguridad de la Información establecidos para el proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido.

La DCSD supervisará que se cumpla con el desarrollo de las auditorías internas a intervalos planificados o cuando ocurran cambios significativos en la puesta en marcha de la seguridad.

La planificación y ejecución de las auditorías internas, serán desarrolladas por la SDSCD y la DSR, estableciendo la frecuencia y los recursos necesarios para ejecutar las auditorías internas.

La SDSCD y la DSR, deberán asignar las responsabilidades respecto a la seguridad de la información, según los roles que les corresponda.

b. Evaluación de riesgos

Para el proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido, se deberá efectuar la gestión de riesgos, teniéndose en consideración tanto las amenazas internas como las externas. Asimismo, se evaluarán e implementarán las opciones de tratamiento del riesgo que permitan mitigar el impacto negativo en los activos de información.

La gestión del riesgo se realizará de acuerdo al Manual de la Gestión Integral del Riesgo definida por el RENIEC.

Los órganos que conforman el proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido, son responsables de realizar la evaluación de los riesgos en el ámbito de sus competencias y según les corresponda, debiendo presentar los resultados de la evaluación a la DCSD y proponer las respectivas opciones para su tratamiento.

Corresponderá a la DCSD en concordancia con la Oficina de Integridad y Riesgos y la Oficina de Tecnología de la Información a cargo del Sistema de Gestión de Seguridad de la Información a nivel institucional, decidir si se acepta el riesgo o se brindan las facilidades necesarias para implementar las opciones de tratamiento que permita evitar o mitigar el impacto de estos riesgos.

c. Control de accesos

Se controlará el acceso a la información confidencial generada durante el proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido, en concordancia con lo establecido en el Plan de Privacidad, la clasificación de información y los resultados de la gestión de riesgos.

La administración del acceso a los usuarios debe considerar que:

- Toda solicitud de acceso físico y lógico, así como la administración de las cuentas de usuario a los activos de información deberá ser realizada conforme a los procedimientos establecidos.
- Sólo se asignarán cuentas de acceso individuales. Si por razones de operación se requiere el uso de una misma cuenta para más de un usuario, deberá ser de conocimiento del Oficial de Seguridad de Información de la DCSD y aprobado por la Dirección correspondiente al área usuaria.

El personal que reciba una cuenta de usuario para el acceso a los activos de información deberá hacer uso adecuado de sus contraseñas de acceso, manteniendo la confidencialidad de la misma, no dejando su estación de trabajo desatendida, solicitando su cambio de contraseña si tiene algún indicio de su vulnerabilidad y seleccionando una contraseña que tenga un nivel adecuado de complejidad. Es responsabilidad del supervisor informar al Oficial de Seguridad de la Información sobre el cumplimiento de estas disposiciones.

Es responsabilidad de los propietarios de los activos de información el clasificar la información (física o digital) de acuerdo a lo indicado en los lineamientos definidos para la clasificación de la información. Asimismo, identificar y agrupar a los usuarios, considerando su necesidad de información para el desarrollo de sus funciones o labores que realizan, con

la finalidad de establecer los niveles de acceso a la base de datos, sistemas y/o aplicativos, centros de datos, infraestructura de procesamiento de información, archivos físicos y electrónicos, de acuerdo con el resultado de la evaluación de riesgos y los requerimientos de la organización.

Con respecto a los accesos de entidades, organizaciones o instituciones externas que requieran acceder a los servicios (de corresponder), se deberá controlar los accesos lógicos proporcionados a dichas entidades estableciendo interfaces seguras entre la red de datos del RENIEC y la red de datos de la entidad externa.

Previo al acceso a los servicios del RENIEC, dichas entidades externas deberán firmar un acuerdo de confidencialidad y un compromiso a salvaguardar la integridad, disponibilidad y confidencialidad de la información que utilice o sea de su conocimiento.

Corresponde a los órganos que conforman el proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido, establecer un proceso periódico de revisiones de los derechos de acceso tanto de su personal como de los usuarios de entidades externas, así mismo, programar revisiones periódicas de las políticas configuradas en su red de datos.

Es responsabilidad del encargado o supervisor de cada órgano o unidad orgánica solicitar en el menor tiempo posible la inactivación de las cuentas de usuario cuando estos ya no presten sus servicios, o cuando el usuario o entidad externa ya no requiera del acceso a la información del RENIEC.

d. Seguridad de personal

Cada órgano o unidad orgánica debe asegurar que el personal, contratista y terceros reciban y comprendan sus responsabilidades respecto al uso y tratamiento de los activos de información, con la finalidad de reducir el riesgo de hurto, fraude o mal uso de la información. Así mismo, deberán asegurar la implementación de controles de seguridad relacionados al personal, antes, durante y finalizado el empleo o servicio brindado dentro del proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido.

Antes del empleo:

- Los perfiles de los puestos deberán ser definidos en base a las funciones que se van a desarrollar y las responsabilidades que les competen.
- La OPH, debe implementar controles para la selección y contratación del personal, a fin de verificar la veracidad de los datos proporcionados por los postulantes, así como sus antecedentes penales y policiales.
- Para los servicios efectuados por terceros, la verificación de los datos del personal la efectuará el proveedor del servicio. El RENIEC se reserva el derecho de verificar dicha documentación.

- Cada una de las personas que presta servicios en el proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido, deben firmar un acuerdo de confidencialidad o un documento de compromiso de aceptación o cumplimiento, según corresponda, para salvaguardar la integridad, disponibilidad y confidencialidad de la información que utilice o sea de su conocimiento.

Durante el empleo:

- Toda persona que presta servicios en el proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido, debe recibir charlas de inducción en materia de Seguridad de la Información.
- Se deben desarrollar actividades de capacitación permanente dirigidas a mantener actualizados los conocimientos del personal respecto al uso y reserva de la información, así como a las políticas y procedimientos relevantes para sus funciones. Estas actividades de capacitación, así como los responsables de efectuarlas deben estar definidas en un Plan o Programa de Sensibilización.
- Para los casos de tercerización de servicios se informará al prestador del servicio cuáles son los criterios que deberá considerar para la seguridad de la información, así como también, se monitoreará y revisará su cumplimiento.
- Todo incumplimiento de la Política de Seguridad de la Información por parte del personal o proveedores, deberá ser informado al Oficial de Seguridad de Información de la DCSD para su análisis, evaluación y comunicación a la OPH, a fin de que ésta proceda a la sanción que corresponda en concordancia con su normativa correspondiente, o en el caso de los proveedores, para su comunicación a la OAF para la sanción que corresponda de acuerdo a la Ley de Contrataciones del Estado o a lo establecido en el contrato.

Finalización del empleo:

- Todo cambio o finalización de funciones deberá realizarse de acuerdo a los procedimientos del RENIEC, incluyendo la entrega de los bienes asignados al personal. De igual modo, cada encargado o supervisor deberá solicitar el retiro de los accesos de su personal a la información o servicios.

La Oficina de Potencial Humano, la Oficina de Administración y Finanzas, y los órganos que conforman el proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido, son los responsables de implementar lo estipulado en la Política de Seguridad de la Información con el personal y proveedores, respectivamente.

e. Seguridad física de las instalaciones

Se deben implementar controles de seguridad física con la finalidad de prevenir accesos no autorizados a los ambientes en que se procesa o resguarda información confidencial, así mismo, evitar el daño o pérdida de los activos de información críticos.

Se deben delimitar los perímetros del ambiente en que se procesa o resguarda la información sensible, y se establecerán los controles físicos de entrada y salida; asimismo, se instalarán controles de seguridad contra incendios, aniegos y otros, que permitan alertar en casos de emergencia.

Los ambientes serán diseñados e implementados adecuadamente para la seguridad del personal y de los recursos. Se deberá; asimismo, establecer controles de acceso a los ambientes, al uso de las llaves de los mismos, y asignar a los responsables respectivos. También, se debe definir e implementar un plan de evacuación en casos de desastre.

Estas políticas de seguridad física se deben considerar también para los ambientes de contingencia.

La OSDN, la OTI, y los órganos que conforman el proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido, son los responsables de implementar las políticas de seguridad física, según les corresponda.

f. Seguridad de comunicaciones y redes

Se deben establecer responsabilidades y procedimientos documentados de operación asociado al procesamiento de información y recursos de comunicaciones, con el objetivo de evitar daños, accesos no autorizados, mal uso de los activos de información, garantizar la seguridad de los datos y la disponibilidad de los servicios utilizados a través de la red del RENIEC y del internet.

En lo posible se segregarán las tareas y se implementará un procedimiento de gestión de cambios, con la finalidad de prevenir modificaciones no autorizadas en los equipos de comunicaciones y redes.

La SDSCD asegurará que los datos disponibles en los repositorios públicos se encuentren protegidos; asimismo, deberá garantizar la disponibilidad de los mismos.

Es responsabilidad de la OTI y los órganos que conforman el proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido, implementar políticas de seguridad de comunicaciones y redes, según les corresponda.

g. Mantenimiento de equipos y su desecho

Se debe asegurar la disponibilidad e integridad de los equipos a través de un adecuado plan de mantenimiento. Se debe elaborar un plan de mantenimiento preventivo especialmente para los equipos críticos, el cual se realizará según el procedimiento establecido por el RENIEC, documentándose los incidentes que ocurran antes, durante y después del mantenimiento.

Antes del desecho o reúso de los equipos se revisará que toda información sensible haya sido removida o sobre escrita, con la finalidad de prevenir el acceso no autorizado a información sensible.

El reemplazo, decomiso, manipulación y desecho, tanto del hardware como del software, se realizará de acuerdo a los criterios establecidos por RENIEC para el correcto uso de los equipos.

La OAF, la OTI y los órganos que conforman el proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido, serán los responsables, según les corresponda, de implementar las políticas de mantenimiento de equipo y su desecho.

h. Control de cambios y configuración

Se debe asegurar un control satisfactorio de todos los cambios realizados a los equipos, software y procedimientos, en lo posible se deberá garantizar la posibilidad de revertir los cambios efectuados sin éxito.

Se deberá realizar y aprobar los cambios en los sistemas y recursos de tratamiento de información, de acuerdo a lo establecido; asimismo, previo al cambio se efectuará un análisis de impacto a los sistemas y procesos, comunicando el cambio a todos los involucrados. Se ha dispuesto que todo cambio o modificación que se realice al sistema sea debidamente documentado, y además que dichas modificaciones se efectúen de preferencia, fuera del horario de atención a los clientes o en horas de menor demanda.

Corresponde a la OTI, y los órganos que conforman el proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido, implementar las políticas asociadas a la gestión de cambios y configuración.

i. Planificación de contingencias

Los órganos que tienen la responsabilidad de desarrollar y proporcionar los servicios de Certificación Digital y la Prestación de Servicios de Valor Añadido, que se brindan a los usuarios, implementarán un Plan de Contingencias a nivel de servicios, que les permita reaccionar ante una posible interrupción en las actividades críticas del proceso y en el tiempo requerido por el RENIEC.

Para establecer el Plan de Contingencias se identificarán procesos críticos para el servicio prestado, los eventos que pueden ocasionar interrupciones en estos procesos, y los planes o acciones que se deberán efectuar para mantener y recuperar las operaciones, así como el periodo en que estos deberán recuperarse.

Se deberá establecer pruebas periódicas del Plan de Contingencias, que permitan evaluar su eficacia y efectuar su actualización, de ser el caso.

Corresponde a los órganos que tienen la responsabilidad de desarrollar y proporcionar los servicios de Certificación Digital y la Prestación de Servicios de Valor Añadido, implementar las políticas de planificación de contingencias.

j. Respuesta a incidentes

Se deberá clasificar, comunicar y atender los incidentes de manera rápida, eficaz y sistemática, a fin de garantizar el restablecimiento del servicio afectado en el menor tiempo posible.

Para el caso de los incidentes que afecten la seguridad de la información, se deberá establecer que toda persona (personal o proveedor) que presta servicios en el proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido, deberá comunicar oportunamente al Oficial de Seguridad de la Información de la DCSD o persona designada por el órgano, cuando se haya detectado o tomado conocimiento del incidente, para que puedan ser atendidos conforme al procedimiento establecido. Adicionalmente, el gestor líder de seguridad de la información de la DCSD deberá llevar un registro de los incidentes de seguridad ocurridos en su ámbito de alcance, monitoreando la implementación de las acciones correctivas o preventivas que ameriten.

La OTI del RENIEC define los lineamientos de la gestión de incidentes y los órganos que conforman el proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido serán los responsables de cumplir con las disposiciones establecidas para la gestión de los incidentes.

k. Auditorías y detección de intrusiones

Se programarán como mínimo auditorías anuales, las cuales se ejecutarán de acuerdo al Plan Anual de Auditoría definido. Al término de la auditoría el área o persona auditada deberá implementar en el menor tiempo posible las acciones correctivas y preventivas identificadas.

Se deberán ejecutar pruebas periódicas de detección de intrusiones, así como, implementar controles que permitan alertar los intentos de acceso no autorizados.

Los sistemas y procesos (manuales o automáticos) deberán contar con registros de auditoría actualizados, los mismos que deben brindar información de la acción ejecutada, la hora, fecha, identificación del personal, software y hardware utilizado, según corresponda.

La DCSD, SDSCD y DSR deberán elaborar su Plan Anual de Auditoría Interna y hacerlo de conocimiento de la DCSD, así como dar a conocer el desarrollo de su ejecución.

Las pruebas periódicas de detección de intrusiones deberán ser programadas y comunicadas a la DCSD. Adicionalmente, los controles de detección de intrusiones deberán ser implementados por la OTI y la SDSCD, según corresponda.

I. Medios de almacenamiento

Se debe asegurar la protección de los documentos, medios informáticos, datos de entrada o salida y documentación del proceso de Registros de Certificación Digital y Servicios Digitales relacionado a los servicios de Certificación Digital y Prestación de Servicios de Valor Añadido, de las ocurrencias como daño, modificación, robo o acceso no autorizado.

Se debe establecer un procedimiento para la administración de los medios de almacenamiento de información, y los controles de seguridad requeridos para el almacenamiento, uso y protección de la información, considerándose también el uso de los medios de almacenamiento removibles, el proceso de eliminación segura de información, la planificación y ejecución de copias de seguridad, así como su proceso de restauración.

La OTI y la SDSCD tendrán bajo su responsabilidad la implementación de la Política de medios de almacenamiento, de acuerdo a sus competencias.

m. Administración de Claves

La SDSCD debe asegurar la confidencialidad de las claves criptográficas e implementará medidas para su protección y los controles requeridos de acuerdo al nivel de seguridad acreditado.

La protección de las claves criptográficas administradas por la SDSCD, se efectuará conforme a lo establecido en el Plan de Seguridad de la Información y a los documentos técnicos de la gestión de llaves de la ECEP y PSVA.

La SDSCD tiene la responsabilidad de implementar lo establecido en el Plan de Seguridad de la Información y en los documentos técnicos de la gestión de las llaves de la ECEP y PSVA.

8. Referencias

- La norma ISO/IEC 27002 “Information technology – Code of practice for information security management” y la norma ISO/IEC 13335 “Information technology - Guidelines for the management of IT Security”.
- Norma Técnica Peruana NTP-ISO/IEC 27001:2022 referida a Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información.
- La norma ISO/IEC 15408 “Information technology – Security techniques - Evaluation criteria for IT security”.