Anexo 09

Política de Seguridad

Política de Seguridad

ECERNEP - ECEP - EREP

Versión: 3.0	Año: 2013	
Elaborado por: Oficial de Seguridad de Información	**Revisado por:** Coordinador de Seguridad de Información Comité para Acreditación - GCRD	**Aprobado por:** Gerente de Certificación y Registro Digital

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

INDICE

1. Objetivo

Establecer el marco general y los lineamientos para la seguridad de la información que administra la Entidad de Certificación Nacional para el Estado Peruano – ECERNEP, Entidad de Certificación para el Estado Peruano - ECEP y Entidad de Registro o Verificación para el Estado Peruano - EREP, del RENIEC; a fin de garantizar la disponibilidad, confidencialidad e integridad de la información durante el desarrollo de las operaciones y acciones que éstas 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 Información de la Gerencia de Certificación y Registro Digital. Teléfono: (01) 315 2700 – (01) 315 4000 anexo 1195. Correo Electrónico: identidaddigital@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.
- 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".
- Resolución Comisión de Reglamentos Técnicos y Comerciales N° 030-2008/CRT-INDECOPI, del 12 de marzo de 2008, que Aprueban las Guías de Acreditación de Entidades de Certificación Digital, Entidades de Registro o Verificación de Datos y Entidades de Prestación de Servicios de Valor Añadido, así como la Guía para la Acreditación del Software de Firmas Digitales.

- Resolución Jefatural N° 265-2010-JNAC/RENIEC, del 30 de marzo de 2010, que aprueba la Directiva DI-288-GI/020 "Lineamientos generales de Seguridad de la Información".
- Resolución Jefatural N° 060-2013/JNAC/RENIEC, del 22 de febrero de 2013, que aprueba la "Política 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 para el personal de la ECERNEP, ECEP-RENIEC y EREP-RENIEC, así como del personal de los distintos órganos del RENIEC que participen en la ejecución de las actividades que son parte del proceso de certificación digital.

La presente política así como las reglas o normas y procedimientos que se deriven de ella, también serán de cumplimiento obligatorio para los proveedores de servicios o terceros de la ECERNEP, ECEP-RENIEC y EREP-RENIEC.

b) Servicios de alcance

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

- EREP–RENIEC: comprende los servicios de 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.
- ECEP–RENIEC: Comprende los servicios de emisión y cancelación de certificados digitales, administración de su ciclo de vida, administración de repositorio y consulta de estado de certificados digitales.

c) Inclusiones de este documento

El presente documento incluye los siguientes aspectos: la evaluación 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 que la ECERNEP, ECEP-RENIEC y EREP-RENIEC realizan.

5. Responsables

- **Responsables de aprobar y apoyar la implementación de la Política de Seguridad ECERNEP - ECEP - EREP**
  - La Gerencia de Certificación y Registro Digital del RENIEC.
- **Responsables de elaborar, efectuar revisiones periódicas, proponer y apoyar la implementación de la Política de Seguridad ECERNEP - ECEP - EREP**
  - El Oficial de Seguridad de Información de la GCRD.
  - El Coordinador de Seguridad de Información de la GCRD.
  - El Comité para la Acreditación ECERNEP, ECEP y EREP de la GCRD.
- **Responsables de implementar la Política de Seguridad ECERNEP - ECEP - EREP**
  - Los órganos del RENIEC involucrados en el proceso de certificación digital, en los aspectos que les correspondan.
- **Responsables de supervisar el cumplimiento de la Política de Seguridad ECERNEP - ECEP - EREP**
  - El Oficial de Seguridad de Información de la GCRD.
  - El Coordinador de Seguridad de Información de la GCRD.
  - Cada Gerente de los órganos del RENIEC involucrados en el proceso de certificación digital.
  - Los Supervisores de Seguridad de Información y Privacidad de Datos de los órganos que conforman la ECEP-RENIEC y EREP-RENIEC.

6. Glosario de términos

- **Activo:** Algo que tenga valor para la organización.
- **Análisis de riesgos:** Uso sistemático de la información para identificar orígenes y estimar el riesgo.
- **Amenaza:** Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización.
- **Control:** Herramienta de la gestión de riesgos, incluido políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal.
- **Evaluación del riesgo:** Proceso general de análisis y evaluación del riesgo.
- **Evento de seguridad de la información:** Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o

red, indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización considerando el riesgo.
- **Identidad digital:** Es el reconocimiento de la identidad de una persona en un medio digital (como por ejemplo Internet) a través de mecanismos tecnológicos seguros y confiables, sin necesidad de que la persona esté presente físicamente.
- **Incidente de seguridad de la información:** Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de negocio y de amenazar la seguridad de la información.
- **Riesgo:** Combinación de la probabilidad de un evento y sus consecuencias.
- **Seguridad de la Información:** Preservación de la confidencialidad, disponibilidad o integridad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, veracidad o confiabilidad también pueden ser consideradas.
- **Tratamiento del riesgo:** Proceso de selección e implementación de medidas o controles para modificar el riesgo.
- **Vulnerabilidades:** Debilidades de seguridad asociadas con los activos de información.

7. Políticas

Genérica

El RENIEC en su calidad de Entidad de Certificación Nacional para el Estado Peruano - ECERNEP, Entidad de Certificación para el Estado Peruano - ECEP y Entidad de Registro o Verificación para el Estado Peruano – EREP, reconoce como su activo principal a la información resultante del proceso de certificación digital, que permite la generación de la identidad digital; en tal sentido, se efectúa el análisis y evaluación de los riesgos, la aplicación de controles y la toma de conciencia 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

El RENIEC ha establecido la siguiente estructura de gestión de la seguridad de la información en el ámbito de la ECERNEP, ECEP y EREP del RENIEC, con la finalidad de implementar en el proceso de certificación digital controles que permitan asegurar la confidencialidad, integridad y disponibilidad de la información.

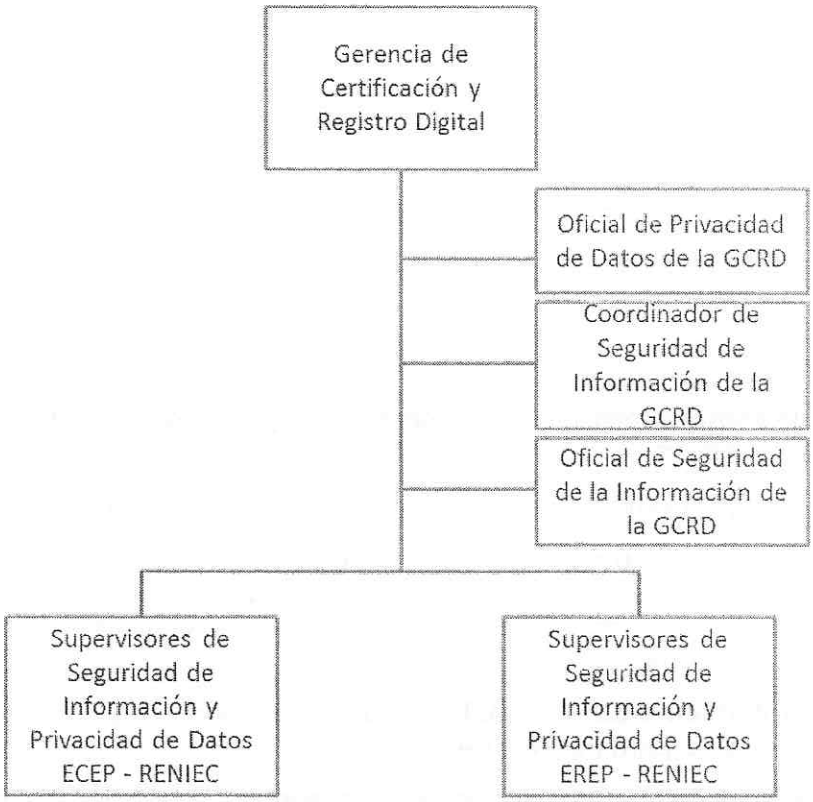

Fig. 1: Estructura de gestión de la Seguridad de la Información en la ECERNEP- EREP- ECEP

El Oficial de Seguridad de Información y el Coordinador de Seguridad de Información de la GCRD, tienen entre sus funciones la elaboración de la Política de Seguridad, así mismo, después de la aprobación de esta política por la Gerencia de Certificación y Registro Digital, esta será publicada a través de la Intranet para conocimiento de todo el personal de los distintos órganos que interviene en el proceso de certificación digital.

La Gerencia de Certificación y Registro Digital también tiene entre sus responsabilidades coordinar el desarrollo de las auditorías internas a intervalos planificados o cuando ocurran cambios significativos en la puesta en marcha de la seguridad; así mismo, asignará las distintas responsabilidades respecto a la Seguridad de la Información a los órganos involucrados en el proceso de certificación digital.

Con la finalidad de garantizar la disponibilidad, confidencialidad e integridad de la información, coordinará la ejecución de revisiones y actualizaciones periódicas de la Política de Seguridad 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 GCRD 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 en la Gerencia de Certificación y Registro Digital con un Oficial de Seguridad de Información quien tiene la responsabilidad de supervisar la implementación de la visión de seguridad de la información, así como de las estrategias, programas, políticas, procedimientos y controles relacionados a la seguridad de la información en el ámbito de la ECERNEP, EREP-RENIEC y ECEP-RENIEC.

Para la planificación y ejecución de las auditorías internas a la ECEP–RENIEC y EREP-RENIEC, la Gerencia de Certificación y Registro Digital cuenta con un Analista de Control Interno, quien en coordinación con los órganos involucrados en el proceso de Certificación Digital establecerá la frecuencia y los recursos necesarios para ejecutar las auditorías internas en el Plan Anual de Auditoria Interna.

Corresponde a los Supervisores de Seguridad de la Información y Privacidad de Datos designados por los órganos que conforman la EREP y ECEP del RENIEC, el verificar el cumplimiento de la Política de Seguridad y el Plan de Seguridad en la ECEP-RENIEC y EREP-RENIEC.

b. Evaluación de riesgos

Para cada proceso vital o crítico que se desarrolla en el ámbito de la EREP-RENIEC y ECEP-RENIEC, se deberá efectuar el análisis y evaluación de riesgos, teniéndose en consideración tanto las amenazas internas como las externas; asimismo, se identificarán, evaluarán e implementarán las opciones de tratamiento del riesgo que permitan mitigar el impacto en los activos de información involucrados en el proceso de certificado digital.

La evaluación y tratamiento del riesgo se realizará de acuerdo a la Metodología de Análisis y Tratamiento del Riesgo definida por la ECEP-RENIEC y EREP-RENIEC.

La EREP-RENIEC y ECEP-RENIEC son responsables de realizar la evaluación de los riesgos en el ámbito de sus competencias, debiendo presentar los resultados de la evaluación a la Gerencia de Certificación y Registro Digital y proponer las respectivas opciones para su tratamiento.

Corresponderá a la Gerencia de Certificación y Registro Digital en concordancia con la Jefatura Nacional, decidir si se acepta el riesgo o se brinda 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 del certificado digital, en concordancia con lo establecido en el

Plan de Privacidad de la ECEP-RENIEC y EREP-RENIEC, así como la información reservada de la ECERNEP y los resultados de la evaluación de riesgos.

La administración del acceso a los usuarios considerará 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 asignará 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 GCRD y aprobado por la Gerencia correspondiente al área usuaria.

El personal que reciba una cuenta de usuario para el acceso a los activos de información de la ECEP-RENIEC y/o EREP-RENIEC deberá hacer uso adecuado de sus contraseñas de acceso, manteniendo la confidencialidad de la misma, no dejando sus estaciones de trabajo desatendidas, solicitando su cambio de contraseña si tiene algún indicio de su vulnerabilidad y seleccionado una contraseña que tenga un nivel adecuado de complejidad; es responsabilidad del supervisor del personal el informar a éste sobre el cumplimiento estas disposiciones y el verificar su cumplimiento.

Es responsabilidad de los propietarios de los activos de información de la ECEP-RENIEC y EREP-RENIEC clasificar la información (física o digital) de acuerdo a lo indicado en los lineamientos definidos para la clasificación de 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 la ECEP-RENIEC, 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, a nivel de puertos para los que se requieren los servicios.

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 la ECERNEP, ECEP-RENIEC y la EREP-RENIEC 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 servicios para la ECERNEP, EREP-RENIEC o ECEP-RENIEC, 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 relacionados al proceso de certificación digital, 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 a la ECERNEP, ECEP-RENIEC y/o EREP-RENIEC.

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 competan.
- La Gerencia de Talento Humano, 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 el caso de quienes tienen roles de confianza, se efectuará la verificación de sus antecedentes crediticios.
- Para los servicios efectuados por terceros, la verificación de los datos 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 la ECERNEP, ECEP-RENIEC y EREP-RENIEC deben firmar un acuerdo de confidencialidad y/o un documento de compromiso 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 la ECERNEP, ECEP-RENIEC o EREP-RENIEC, recibirá charlas de inducción en materia de Seguridad de la Información.
- Se deben desarrollar actividades de capacitación continua 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 estarán definidas en el Plan de Capacitación.

- 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 parte del personal o proveedores, deberán ser informadas, por el personal que tome conocimiento del hecho, al Oficial de Seguridad de Información de la GCRD para su análisis, evaluación y comunicación a la Gerencia de Talento Humano, 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 Gerencia de Administración 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 accesos a la información o servicios de la ECERNEP, ECEP-RENIEC y EREP-RENIEC de su personal.

La Gerencia de Talento Humano, la Gerencia de Administración, y los órganos que conforman la ECERNEP, ECEP-RENIEC y EREP-RENIEC, son los responsables de implementar lo estipulado en la Política de Seguridad con el personal y proveedores, respectivamente.

e. Seguridad física

La ECERNEP, ECEP-RENIEC y EREP-RENIEC 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 perdida de los activos de información críticos que intervienen en el proceso de certificación digital.

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 de los recursos que albergan y del personal. Se deberá, así mismo, establecer controles de acceso a los ambientes, al uso de las llaves de los mismos, y asignar a los responsables respectivos. Así mismo, 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 Oficina de Seguridad y Defensa Nacional, y los órganos que conforman la ECERNEP, ECEP-RENIEC y EREP-RENIEC, son los responsables de implementar las políticas de seguridad física.

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 e implementará un procedimiento de gestión de cambios con la finalidad de prevenir modificaciones no autorizadas en los equipos de comunicaciones y redes.

La ECEP-RENIEC asegurará que los datos disponibles en los repositorios públicos se encuentren protegidos, así mismo, deberá garantizar la disponibilidad de los mismos.

Es responsabilidad de la Gerencia de Tecnología de la Información y los órganos que conforman la ECERNEP, ECEP-RENIEC y EREP-RENIEC, el implementar las políticas de seguridad de comunicaciones y redes.

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. Antes de su 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.

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.

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

La Gerencia de Administración, la Gerencia de Tecnología de la Información y los órganos que conforman la ECERNEP, ECEP-RENIEC y EREP-RENIEC, serán los responsables de implementar las políticas de mantenimiento de equipo y su desecho. Así mismo, corresponde a la

Gerencia de Tecnología de la Información y a la ECEP-RENIEC el efectuar los mantenimientos de los equipos de su competencia.

h. Control de cambios y configuración

La ECEP-RENIEC y EREP-RENIEC deben 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; así mismo, 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 Gerencia de Tecnología de la Información, y los órganos que conforman la ECERNEP, ECEP-RENIEC y EREP-RENIEC, implementar las políticas asociadas a la gestión de cambios y configuración.

i. Planificación de contingencias

La ECEP-RENIEC y EREP-RENIEC implementarán un Plan de Contingencias a nivel de servicios, que les permita reaccionar ante una posible interrupción en las actividades críticas del proceso de certificación digital, y en el tiempo requerido por el RENIEC.

Para establecer el Plan de Contingencias se identificarán procesos críticos para el servicio prestado por la ECEP-RENIEC y EREP-RENIEC, 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 en un lugar alternativo, que permitan evaluar su eficacia y efectuar su actualización.

Corresponde a los órganos que conforman la ECERNEP, ECEP-RENIEC y EREP-RENIEC, 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 la ECERNEP, ECEP-RENIEC y EREP-RENIEC deberá comunicar oportunamente al Oficial de Seguridad de Información de la GCRD o persona designada, cuando se haya detectado o tomado conocimiento del incidente. Adicionalmente, los Supervisores de Seguridad de la Información y Privacidad de Datos, tanto de la ECEP-RENIEC como de la EREP-RENIEC, deberán 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.

Los órganos que conforman la ECERNEP, ECEP-RENIEC y EREP-RENIEC serán los responsables de implementar la política de respuesta a incidentes.

k. Auditorías y detección de intrusiones

Se programarán como mínimo auditorías semestrales, las cuales se ejecutarán de acuerdo al Plan Anual de Auditoría. 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, como hora, fecha, identificación del personal, software y hardware utilizado, según corresponda.

Corresponde al Analista de Control Interno de la Gerencia de Certificación y Registro Digital elaborar el Plan Anual de Auditoría Interna y a la Gerencia de Certificación y Registro Digital aprobarlo, y a los órganos que conforman la ECERNEP, ECEP-RENIEC y EREP-RENIEC brindar las facilidades necesarias para su ejecución. Las pruebas periódicas de detección de intrusiones para la ECEP-RENIEC y EREP-RENIEC serán programadas en el Plan de Auditoría Interna. Adicionalmente, los controles de detección de intrusiones deberán ser implementados por la Gerencia de Tecnología de la Información y la ECEP-RENIEC según corresponda.

Medios de almacenamiento

Se asegurará la protección de los documentos, medios informáticos, datos de entrada o salida y documentación del proceso de certificación digital, de las ocurrencias como daño, modificación, robo o acceso no autorizado.

La ECEP-RENIEC y EREP-RENIEC deben establecer el 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 Gerencia de Tecnología de la Información y la ECEP-RENIEC, tendrán bajo su responsabilidad la implementación de la Política de Medios de Almacenamiento de acuerdo a su competencia.

m. Administración de Claves

La ECERNEP y ECEP-RENIEC deben asegurar la confidencialidad de claves criptográficas e implementarán para su protección los controles requeridos de acuerdo al nivel de seguridad acreditado.

La protección de las claves criptográficas administradas por la ECERNEP, y las administradas por la ECEP-RENIEC y EREP-RENIEC correspondientes a entidades finales, se efectuará conforme a lo establecido en el Plan de Seguridad y Administración de Claves.

Los órganos que conforman la ECERNEP, EREP-RENIEC y ECEP-RENIEC tiene la responsabilidad de implementar lo establecido en el Plan de Seguridad y Administración de Claves.

8. Referencias

- La norma ISO/IEC 17799 "Information technology – Code of practice for information security management" y la norma ISO/IEC TR13335 "Information technology - Guidelines for the management of IT Security".
- La norma ISO/IEC 27001:2005 "Information technology - Security techniques - Information security managementsystems - Requirements".
- La norma ISO/IEC 15408 "Information technology – Security techniques - Evaluation criteria for IT security".