DIRECTIVA

SEGURIDAD INFORMÁTICA DE LA RED DEL RENIEC

RESOLUCIÓN SECRETARIAL N° 94 -2018/SGEN/RENIEC		
DI-328-GTI/022	VERSIÓN: 04 N° PÁGINAS: 33	FECHA DE APROBACIÓN 09 JUL. 2018

INDICE

I. OBJETIVO

Establecer las normas y lineamientos que aseguren los niveles de protección y control de acceso a los recursos informáticos dentro de la red, para mantener la confidencialidad, integridad y disponibilidad de la información del Registro Nacional de Identificación y Estado Civil - RENIEC, reduciendo los riesgos de incidentes de seguridad de la red, así como del hardware y software involucrados.

II. ALCANCE

La presente Directiva es administrada por la Gerencia de Tecnología de la Información, a través de la Sub Gerencia de Operaciones Telemáticas y es de aplicación obligatoria para todas las áreas del RENIEC.

III. BASE LEGAL

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

3.2 **Ley N° 27658,** Ley Marco de Modernización de la Gestión del Estado, del 30 de enero de 2002.

3.3 **Ley N° 28493,** Ley que regula el uso del correo electrónico comercial no solicitado (SPAM), del 12 abril de 2005, y sus modificatorias

3.4 **Ley N° 28716,** Ley de Control Interno de las Entidades del Estado, del 18 de abril de 2006.

3.5 **Decreto Supremo N° 0043-2003-PCM,** aprueba Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, del 24 de abril de 2003 y sus modificatorias.

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

3.7 **Resolución de Contraloría N° 320-2006-CG**, aprueba Normas de Control Interno del 03 de noviembre de 2006.

3.8 **Resolución Ministerial N° 073-2004-PCM,** aprueba la "Guía para a la Administración Eficiente de Software Legal en la Administración Pública", del 17 de marzo de 2004.

3.9 **Resolución Ministerial N° 004-2016-PCM,** aprueban 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,** aprueba la modificación del artículo 5 de la Resolución Ministerial N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información, del 21 de junio de 2017.

3.11 **Resolución Comisión de Reglamentos Técnicos y Comerciales N° 001-2007/INDECOPI-CRT,** aprueba la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de seguridad de la información. 2ª. Edición, del 22 de enero de 2007.

3.12 **Resolución Jefatural N° 207-2002-INEI,** aprueba la Directiva N° 010-2002-INEI/DTNP "Normas Técnicas para la Asignación de Nombres de Dominio de las entidades de la Administración Pública", del 11 de julio de 2002 y sus modificatorias.

3.13 **Resolución Jefatural N° 088-2003-INEI,** aprueba la Directiva N° 005-2003-INEI/DTNP "Normas para el uso del servicio de correo electrónico en las Entidades de la Administración Pública", del 03 de abril de 2003.

3.14 **Resolución Jefatural N° 073-2015/JNAC/RENIEC,** aprueba la Política de Seguridad de la Información y los Objetivos de Seguridad de la Información del RENIEC, del 30 de Marzo del 2015.

3.15 **Resolución Jefatural N° 073-2016/JNAC/RENIEC,** aprueba el Reglamento de Organización y Funciones y la Estructura Orgánica del Registro Nacional de Identificación y Estado Civil, del 01 de junio del 2016.

3.16 **Resolución Jefatural N° 069-2017-/NAC/RENIEC,** aprueba la reconstitución del Comité de Gestión de Seguridad de la Información del Registro Nacional de Identificación y Estado Civil, del 22 de mayo de 2017.

3.17 **Resolución Secretarial N° 000055-2017/SGEN/RENIEC,** 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.

IV. DEFINICIÓN DE TERMINOS

4.1 **Autenticación**

Es el proceso de detectar y comprobar la identidad digital del remitente de una comunicación electrónica.

4.2 **Bloqueadores de Puertos**

Dispositivo físico usado para evitar la conexión o desconexión de un terminal.

4.3 **Centro de Cómputo**

Es la ubicación donde se concentran los recursos necesarios para el procesamiento de la información de la Institución.

4.4 **Confidencialidad**

Es un principio de la seguridad de la información que impide la divulgación de información a individuos, entidades o procesos no autorizados.

4.5 **Contraseña**

Conjunto de letras, números y símbolos utilizadas para autenticar usuarios en un sistema informático.

4.6 **Criptografía**

La criptografía es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet.

4.7 **Disponibilidad**

Es un principio de la seguridad de la información que busca garantizar que los usuarios autorizados tengan acceso a la información en el momento que la requieran.

4.8 **Dispositivos de Almacenamiento**

Los dispositivos de almacenamiento son elementos técnicos destinados a proveer de espacio físico para albergar archivos.

4.9 **Dispositivos físicos de red**

Dispositivo físico usado para evitar la conexión o desconexión de un terminal de red.

4.10 **Denegación de Servicio (DoS - Denial of Services)**

Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

4.11 **Denegación de Servicio Distribuido (DDoS - Distributed Denial of Services)**

Es un ataque informático de denegación de servicio a computadoras ocasionando que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de conectividad por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

4.12 **Estación de Trabajo**

Área destinada para que un usuario de la red pueda acceder mediante dispositivos de red (Pc´s, laptop, tabletas, teléfono, etc.).

4.13 **Firewall**

También conocido como cortafuegos, es parte de un sistema o de una red que está diseñado para controlar todas las comunicaciones entrantes y salientes. Su función principal es denegar el acceso no autorizado a la red.

4.14 **Firewall de Siguiente Generación**

Es un Firewall con mayores funcionalidades de protección, tales como: Prevención de Intrusos, Antivirus, Antibot, Filtrado URL, Control de Aplicaciones, VPN, Acceso a móviles, Antispam, entre otros.

4.15 **Gusanos**

Son programas capaces de ejecutarse y propagarse por sí mismo a través de las redes informáticas, algunas veces portan virus, otras veces aprovechan los defectos o brechas de seguridad que presentan los sistemas. El daño que pueden causar es considerable.

4.16 **Hacking**

Actividad de un "hacker", hacker es todo aquel experto informático que utiliza sus conocimientos técnicos para descubrir debilidades de un sistema, normalmente asociado a la seguridad.

4.17 **Hardware**

Equipamiento tecnológico constituido por equipos portátiles, equipos de escritorio, discos, equipos de comunicación, servidores, etc.

4.18 **Integridad**

Es un principio de la seguridad de la información que busca mantener los datos libres de modificaciones no autorizadas. La integridad garantiza que los datos permanezcan inalterados excepto cuando sean modificados por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad.

4.19 **Incidente Informático**

Evento único o una serie de eventos no deseados o inesperados que compromete las operaciones y amenazan la seguridad de la información del proceso o del área.

4.20 **IP (Protocolo Internet)**

Es un protocolo de comunicación de datos digitales, cuya función es el envío de paquetes de datos tanto a nivel local como a través de redes.

4.21 **LAN (Local Area Network)**

Red de Área Local, es una red de computadoras que abarca un área reducida a un local o un edificio.

4.22 **Malware**

Se define como software malicioso que cubre un amplio rango de software hostil como son los virus, gusanos, caballos de troya, etc., capaces de causar daños o alteraciones del sistema operativo, archivos, u otros componentes de computadoras y redes informáticas.

4.23 **Media**

Dispositivo que contiene el instalador de un sistema operativo, aplicación o programa puede ser CD, DVD, Blu-ray USB, etc.

4.24 **Mesa de Ayuda**

Conjunto de recursos tecnológicos y humanos, para gestionar incidencias y requerimientos, relacionados a las Tecnologías de la Información y la Comunicación (TIC), de manera integral, con escalamiento a las áreas especializadas de TI, siendo el objetivo principal la resolución de incidentes.

4.25 **No repudio (Evitar el rechazo)**

Evitar el repudio de información constituye la garantía de que ninguna de las partes involucradas pueda negar en el futuro una operación realizada.

4.26 **Protocolo**

Conjunto de reglas conocidas y respetadas que en los extremos de un enlace de telecomunicaciones regulan las transmisiones en todos los sentidos posibles.

4.27 **Recursos Informáticos**

Es el equipamiento de hardware tales como: computadoras, servidores, impresoras, escáneres, etc., y herramientas de software, ya sean éstos programas de terceros, herramientas de internet o software desarrollados dentro de una organización.

4.28 **Responsabilidades**

Define las instancias y a los funcionarios responsables de cumplir y hacer cumplir lo dispuesto en la directiva, en los diferentes niveles de la institución.

Las responsabilidades son de difusión, asistencia técnica, implementación, supervisión, evaluación y aplicación según corresponda, respecto al contenido de la directiva.

4.29 **Seguridad de la Información**

Es el conjunto de medidas que permiten resguardar y proteger la información buscando mantener la confidencialidad, disponibilidad e integridad de los activos de información.

4.30 **Seguridad Informática**

Es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático.

4.31 **Soporte Técnico**

Servicio que brinda la Sub Gerencia de Soporte Técnico Operativo a todos usuarios de la institución. Cuenta con herramientas en hardware y software que le permite colaborar en la resolución de cualquier tipo de problemas.

4.32 **Software de Gestión de Incidentes**

Herramienta Informática de la Sub Gerencia de Soporte Técnico Operativo (SGSTO) que permite gestionar los requerimientos e incidencias de manera oportuna, con el apoyo de las áreas especializadas de TI.

4.33 **SPAM**

Es un correo electrónico no deseado y no solicitado. Estos mensajes son normalmente enviados a través de listas de correo invisibles o grupos de noticias que saturan con propaganda de todo tipo de productos o servicios. Muchos de estos mensajes vienen infectados de virus, gusanos y caballos de Troya.

4.34 **Súper Usuario (Administrador de Usuarios)**

Usuario que posee los más altos privilegios en un determinado sistema.

4.35 **VPN (Virtual Private Network)**

Red Privada Virtual, es una extensión de una red privada a través de una red pública como internet. Se establece una conexión virtual punto a punto mediante el uso de conexiones dedicadas, encriptación, o una combinación de ambos.

4.36 **Vulnerabilidad informática**

Es un punto débil del software que permite que un atacante comprometa la integridad, disponibilidad o confidencialidad del software. Algunas de las vulnerabilidades más severas permiten que los atacantes ejecuten código arbitrario, denominadas vulnerabilidades de seguridad, en un sistema comprometido.

4.37 **WAN (Wide Área Network)**

Red de Área Amplia, es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física, proveyendo servicios a una zona, región o país.

V. RESPONSABILIDADES

5.1 Es responsabilidad de la Gerencia de Tecnología de la Información (GTI) velar por el cumplimiento de la presente Directiva.

5.2 La Sub Gerencia de Operaciones Telemáticas (SGOT) es responsable de la administración de la seguridad informática (Seguridad Perimetral e Interna), así como de la toma de acciones que sean necesarias para asegurar su confiabilidad, en función a los recursos y capacidades disponibles.

5.3 Es responsabilidad de la Sub Gerencia de Soporte Técnico Operativo (SGSTO) la instalación y configuración en las estaciones de trabajo, y su entrega a los usuarios finales con versiones actualizadas del sistema operativo y del antivirus; cualquier cambio a la configuración de algún equipo debe ser autorizado por la GTI y ejecutado por la Sub Gerencia de Soporte Técnico Operativo.

5.4 La Sub Gerencia de Operaciones Telemáticas, en coordinación con los Administradores de Servidores de la Sub Gerencia de Soporte Técnico Operativo y los analistas de la Sub Gerencia de Ingeniería Software (SGIS), determinan la estrategia de seguridad a implementar en la instalación de antivirus y actualizaciones de sistema operativo en los servidores que soportan aplicaciones y servicios críticos.

5.5 Es responsabilidad del operador de turno del Centro de Cómputo velar por la integridad física del Centro de Cómputo.

5.6 Es responsabilidad del Administrador de cada Agencia, Oficina Registral Oficinas Registrales Auxiliares – ORAS y la Oficina de la Entidad de Registro del Estado Peruano (EREP), velar por la integridad física de los equipos de cómputo instalados en su sede.

5.7 Es responsabilidad del usuario final reportar a Mesa de Ayuda, a través del *"Software de Gestión de Incidentes"*, cualquier anomalía física y/o lógica en los sistemas y/o equipos informáticos a su cargo, debiendo otorgar las facilidades necesarias, en caso amerite, para que el servidor civil especializado de la GTI efectúe las acciones correctivas que permitan solucionar los incidentes reportados.

5.8 Es responsabilidad del usuario final cumplir con las disposiciones señaladas en el presente documento. En caso de incumplimiento, la Sub Gerencia de Operaciones Telemáticas comunica a la GTI, mediante informe técnico con copia a la Gerencia de Talento Humano (GTH), para la evaluación y acciones pertinentes.

5.9 Es responsabilidad de la Oficina de Seguridad y Defensa Nacional (OSDN) de la seguridad de la información de la institución de acuerdo al Reglamento de Organización y Funciones (ROF).

5.10 Es responsabilidad de las unidades orgánicas que contratan servicios de alquiler de estaciones de trabajo a terceros, comunicar a la Sub Gerencias de Soporte Técnico Operativo y de Operaciones Telemáticas para que se apliquen las políticas de seguridad correspondientes.

VI. DISPOSICIONES GENERALES

6.1 DE LA SEGURIDAD DE LOS RECURSOS INFORMÁTICOS

6.1.1 Los recursos informáticos y el uso correcto de la información crítica o sensible del RENIEC permiten el normal desempeño de las actividades de la entidad.

6.1.2 La instalación y configuración de los recursos informáticos es responsabilidad del servidor civil de la GTI, cualquier cambio a la configuración de los equipos debe ser autorizado por la GTI.

6.2 DE LA SEGURIDAD FÍSICA Y DEL ENTORNO

6.2.1 Los equipos de comunicación de la infraestructura del RENIEC están instalados dentro de gabinetes o cuartos de comunicaciones cerrados con llave y con sistema de alimentación continua de energía en las diferentes Sedes, Agencias, Oficinas Registrales, Jefaturas Regionales, Oficinas Registrales Auxiliares – ORAS y las Oficinas de la Entidad de Registro del Estado Peruano (EREP).

6.2.2 Los equipos y servidores de la infraestructura informática del RENIEC, están ubicados en los Centros de Cómputo de las sedes principales de la institución (Sede Operativa, Sede Administrativa y Sede San Borja).

6.2.3 Para el acceso de los usuarios al Centro de Cómputo se tienen controles biométricos y tarjeta de aproximación, así como una bitácora para el control manual de ingresos y salidas.

6.3 DEL CONTROL DE ACCESO A LOS SERVICIOS DE RED Y SEGURIDAD DE LOS DATOS

6.3.1 Los dispositivos o recursos de telecomunicaciones en el tratamiento de la información tienen configuradas rutas establecidas (pre-definidas) y dominios lógicos de acceso al sistema, los cuales están segmentados y divididos, tomando como premisa el control de acceso a la red y los objetivos principales de la Institución.

6.3.2 Se aplican medidas de control a los dispositivos de la red para su protección y acceso, para evitar que usuarios no autorizados puedan modificar las configuraciones establecidas.

6.3.3 Los equipos para servicios de Telefonía, Videoconferencia y Videovigilancia IP se encuentran protegidos con dispositivos bloqueadores de puerto físicos, para garantizar la seguridad de la infraestructura de cableado estructurado.

6.3.4 La creación de una cuenta de acceso al dominio interno de la institución, es factible para todos los servidores civiles del RENIEC al momento de adquirir vínculo laboral. El área responsable a la que pertenece el servidor civil debe solicitar el alta del perfil de dominio de acuerdo a la DI-327-GTI/021 "Servicio de Comunicación para Usuarios Finales", numeral 7.1.1 Del Alta del Servicio.

6.3.5 El acceso a los servicios y privilegios de la red (correo electrónico, internet, mensajería instantánea interna, telefonía IP, entre otros) debe ser solicitado por el gerente del área usuaria, al que pertenece el usuario, de acuerdo a la DI-327-GTI/021 "Servicios de Comunicación para Usuarios Finales".

6.3.6 Para acceder al Sistema Operativo, se tiene controladores de Dominio que autentican a los equipos y usuarios cuando éstos inician una sesión e ingresan a la red del RENIEC; esta información se encuentra registrada en cada Catálogo Global del Directorio Activo, la cual permite el control y autenticación.

6.3.7 La conexión será validada sólo si el usuario ha ingresado todos los datos solicitados: usuario y contraseña. Adicionalmente se cuenta con la autenticación de doble factor mediante el uso del DNIe.

6.3.8 Está permitido compartir carpetas dentro de la red para fines estrictamente laborales, el usuario que comparta una carpeta se hace responsable de la información contenida en ella y de los privilegios que otorgue a los usuarios que está compartiendo.

6.3.9 La conexión por escritorio remoto (RDP) a las estaciones de trabajo dentro de la red está permitido únicamente al personal de la GTI.

6.4 DE LAS CONTRASEÑAS Y SEGURIDAD

6.4.1 Las contraseñas representan un factor fundamental de la seguridad de los recursos informáticos, siendo la primera línea de protección básica para el usuario y para la red.

6.4.2 La cuenta de usuario y su contraseña es de carácter personal e intransferible, está prohibido compartir a terceras personas. Por lo tanto se prohíbe solicitar el reseteo de la contraseña de una cuenta de dominio distinto a su titular.

6.4.3 Para la autenticación con el DNIe, se requiere previamente asociar el certificado digital contenido en el chip del DNIe con el perfil de dominio del usuario.

6.5 DE LA GESTION DE CUENTAS Y CLAVES DE SÚPER USUARIO

6.5.1 Por los privilegios que poseen los súper usuarios, existe un estricto control para la gestión de las cuentas y sus respectivas claves de acceso a cada uno de los sistemas de información administrados por la Gerencia de Tecnología de la Información.

6.5.2 Como máximo se tienen dos cuentas de súper usuario para cada sistema de información o plataforma tecnológica.

6.6 DE LA PROTECCIÓN CONTRA ATAQUES INFORMÁTICOS, VIRUS, SOFTWARE MALICIOSO Y SIMILARES

6.6.1 La Sub Gerencia de Operaciones Telemáticas garantiza la seguridad informática del Registro Nacional de Identificación y Estado Civil - RENIEC.

6.6.2 Para garantizar la seguridad informática, inviolabilidad e integridad de la información contenidos en equipos cómputo, servidores u otros dispositivos, que conforman el patrimonio activo de la institución a nivel nacional, se cuenta con soluciones de seguridad informática como: antivirus, antimalware, antispam, filtro de contenido, firewalls de siguiente generación IPS, firewall de aplicaciones web y similares.

6.7 DE LA SEGURIDAD EN LA TRANSMISIÓN DE DATOS Y DOCUMENTOS ELECTRÓNICOS

6.7.1 La seguridad de la transmisión de datos en la red del RENIEC está garantizada por la Sub Gerencia de Operaciones Telemáticas en coordinación con los proveedores del servicio de transmisión de datos.

6.7.2 Los dispositivos de red, que interconectan toda nuestra infraestructura tecnológica a nivel nacional, están configurados con rutas establecidas (pre-definidas) y dominios lógicos que encaminan el tráfico de la red y garantizan que los datos lleguen a su destino final.

6.7.3 Se garantiza la transmisión de la información de manera segura y sin interrupciones a través de medios de fibra óptica y radio enlaces con canales cifrados.

6.8 DEL USO DE LOS CONTROLES CRIPTOGRÁFICOS

6.8.1 Se aplican controles criptográficos con el objetivo de asegurar la confidencialidad, autenticidad y/o integridad de la información.

6.8.2 Las claves criptográficas deben estar disponibles operativamente, tanto tiempo como lo requiera la información correspondiente.

6.9 DE LAS VULNERABILIDADES TÉCNICAS

6.9.1 La Sub Gerencia de Operaciones Telemáticas ejecuta el análisis de vulnerabilidades a las aplicaciones, servicios web y a los sistemas operativos.

6.9.2 Se realiza el análisis de vulnerabilidades a todas las aplicaciones o servicios web antes del pase a producción.

6.9.3 Las Sub Gerencias de la Gerencia de Tecnología de la Información elaboran un plan para corregir las vulnerabilidades encontradas según su criticidad.

VII. DISPOSICIONES ESPECÍFICAS

7.1 DE LA SEGURIDAD DE LOS RECURSOS INFORMÁTICOS

7.1.1 ÁREAS SEGURAS

7.1.1.1 Para el acceso físico y/o lógico de los recursos informáticos se ha establecido lo siguiente:

a. **Las áreas y el entorno donde se encuentran:** Son áreas seguras y los entornos están protegidos por perímetros de seguridad definidos, con barreras de seguridad, controles de entrada y acceso apropiados.

b. **Seguridad de los equipos:** Evitar pérdidas, daños o comprometer la actividad y continuidad de equipos de cómputo.

c. **Controles Generales:** Prevenir la exposición a riesgo o robos de información y de los recursos de tratamiento de información.

d. **Control de acceso:** Controlar el acceso a la información en base a los requisitos de seguridad y requerimientos de función.

e. **Gestión de accesos de usuarios:** Evitar accesos no autorizados a los sistemas de información. Esto contempla la supervisión de los accesos.

f. **Control de acceso a la red:** Controlar el acceso a los servicios para no comprometer la seguridad de las redes internas y externas.

g. **Control de acceso al Sistema Operativo:** Evitar accesos no autorizados a los computadores.

h. **Control en la identificación y autenticación de usuario:** Identificador único y exclusivo para uso de los servidores civiles, a fin de manifestarse y auditarse las actividades de cada responsable particular.

7.1.1.2 Los equipos de cómputo y servidores, son para el uso exclusivo para el cual han sido asignados a cada servidor civil. Se prohíbe el uso para fines comerciales o actividades no relacionadas al RENIEC.

7.1.1.3 Los servidores civiles están prohibidos de atentar contra la seguridad de los recursos informáticos del RENIEC, así como detener su operatividad, o privar de acceso a usuarios autorizados a estos recursos.

7.1.1.4 La copia del software protegido por derecho de autor, ya sea en medios magnéticos, óptico de otra índole, se encuentra prohibido.

7.1.1.5 La copia de software de propiedad del RENIEC debe ser para fines de respaldo, y en caso esté permitido por la licencia del software.

7.1.1.6 La instalación de software en equipos cómputo del RENIEC que no haya sido autorizado por la Gerencia de Tecnología de la Información, está prohibido.

7.2 DE LA SEGURIDAD FÍSICA Y DEL ENTORNO

7.2.1 DE LAS ESTACIONES DE TRABAJO

7.2.1.1 La Sub Gerencia de Operaciones Telemáticas realiza el cableado estructurado de la red de acuerdo a un plano de distribución aprobado por la Sub Gerencia de Servicios Generales y el área usuaria.

7.2.1.2 El cambio arbitrario de la ubicación y/o mudanza de las estaciones de trabajo sin autorización de la Sub Gerencia de Operaciones Telemáticas se encuentra prohibido. Para realizar cambios de ubicación de los puntos de red se debe coordinar, a través de correo electrónico, con la Sub Gerencia de Operaciones Telemáticas para la verificación, evaluación y autorización correspondiente.

7.2.1.3 La Sub Gerencia de Operaciones Telemáticas garantiza la conectividad de la estación de trabajo siempre y cuando se mantenga en la ubicación definida de acuerdo al plano de distribución.

7.2.2 DE LOS EQUIPOS DE COMUNICACIÓN QUE SE UBICAN EN EL CENTRO DE CÓMPUTO

7.2.2.1 Los recursos informáticos y de comunicaciones que se encuentran en el Centro de Cómputo cuentan con medidas de seguridad tales como: servicio de alimentación ininterrumpida, flujo de alimentación estabilizada, sistema de refrigeración, control de acceso físico y/o biométrico para el ingreso de los servidores civiles y/o proveedores autorizados.

7.2.2.2 Para el ingreso al Centro de Cómputo se tienen tres tipos de accesos:

a. **Directo:** Se otorga al servidor civil que por naturaleza de sus funciones tiene acceso permanente a las instalaciones del Centro de Cómputo y no requiere autorización expresa. Ejemplo: los operadores de la Sub Gerencia de Soporte Técnico Operativo.

b. **Autorizado:** Se otorga al servidor civil que requiere ingresar al Centro de Cómputo eventualmente, el cual figura en una lista autorizada, debiéndose registrarse en la Bitácora de Control de Acceso del Centro de Cómputo.

c. **Especial:** Se otorga excepcionalmente al servidor civil que no figura en la lista autorizada y por lo tanto requiere autorización expresa del responsable del Centro de Cómputo. A su vez debe registrar su ingreso en la Bitácora de Control de Acceso del Centro de Cómputo.

7.2.2.3 El Operador del Centro de Cómputo es el encargado de registrar, supervisar, custodiar y asistir al visitante. En él recae la responsabilidad del actuar del visitante dentro del área en mención. La presencia de un operador en el Centro de Cómputo debe ser permanente para el monitoreo de la infraestructura TI y *facilities* (UPS, Aire acondicionado, control de accesos, etc.) a fin de garantizar las actividades de emergencia ante cualquier eventualidad.

7.2.3 DE LOS EQUIPOS DE COMUNICACIONES INSTALADOS EN LOS RACKS DE COMUNICACIONES DE CADA PISO EN SEDES Y OFICINAS REGISTRALES

7.2.3.1 Los equipos de comunicaciones se encuentran protegidos tanto física, electrónica, como eléctricamente, por medios de protección conocidos (Gabinete cerrado con llave y Sistema de Alimentación Ininterrumpida).

7.2.3.2 El administrador de cada Agencia, Oficina Registral y Oficina de la Entidad de Registro del Estado Peruano (EREP) es responsable por la integridad física de los equipos de comunicación a su cargo. Se prohíbe la instalación y manipulación de equipos sin autorización de la GTI.

7.2.3.3 La Sub Gerencia de Operaciones Telemáticas es responsable de llevar el inventario de todos los equipos de comunicaciones en el Sistema de Control Patrimonial en coordinación con la Sub Gerencia de Control Patrimonial. El

traslado de los equipos de comunicaciones se debe realizar con la autorización de la Sub Gerencia de Operaciones Telemáticas, quien evalúa los riesgos, aprueba y coordina las acciones a realizar para garantizar el normal funcionamiento de los equipos de comunicaciones.

7.3 DEL CONTROL DE ACCESO A LOS SERVICIOS DE RED Y SEGURIDAD DE LOS DATOS

7.3.1 DEL CONTROL DE ACCESOS A LOS SERVICIOS DE RED

7.3.1.1 La cuenta de dominio tiene la siguiente estructura: La letra inicial del nombre del usuario seguido del apellido paterno. En caso de existir dos cuentas de dominio similares en el directorio activo, se añade progresivamente las letras del apellido materno hasta conseguir una nueva cuenta de dominio no repetida.

7.3.1.2 Al crearse una cuenta de dominio, se establece una contraseña por defecto, luego del primer inicio de sesión el sistema fuerza a cambiarla. El usuario elige la nueva contraseña con el formato y sintaxis señalada en el numeral 7.4.2 y desde ese momento y cada vez que la renueve asume la responsabilidad sobre la inviolabilidad de la contraseña.

7.3.1.3 La Sub Gerencia de Operaciones Telemáticas establece políticas de restricción de acceso por perfiles, restringiendo la instalación de software no autorizado, acceso al panel de control y otras opciones de configuración de los computadores.

Cuando el usuario requiera una excepción temporal a las restricciones mencionadas, el responsable del área solicita la excepción mediante la herramienta "Software de Gestión de Incidentes" de Soporte Técnico, dirigido a la Sub Gerencia de Operaciones Telemáticas. Los Gerentes, Jefes de Oficina, Asesores y los servidores civiles de la GTI están exceptuados de estas restricciones.

7.3.1.4 El uso de las cuentas del directorio activo genera eventos que se registran en las estaciones de trabajo utilizadas. Los eventos se clasifican de acuerdo a su importancia en los siguientes niveles:

a. ALTA, se almacenan hasta por un periodo de seis meses.
b. MEDIA, se almacenan hasta por un periodo de tres meses.
c. BAJA, se almacenan hasta por un periodo de un mes.

Se registran los siguientes parámetros:

d. Identificación del usuario.
e. Fecha y hora de conexión y desconexión.
f. Identificación del terminal o el lugar si es posible.

g. Registro de los intentos aceptados y rechazados de acceso al sistema.

h. Registro de los intentos aceptados y rechazados de acceso a datos y otros recursos.

7.3.1.5 Se aplican políticas de seguridad de capa 2 en los equipos de acceso a red (switches), con el fin de evitar que dispositivos físicos (PC, Laptops de usuarios del RENIEC y/o invitados) no autorizados ingresen a la red LAN. La conexión a red LAN se habilita por una única interfase en un equipo de acceso y está limitada a uno o dos dispositivos físicos, dependiendo del perfil de usuario. Cuando se requiera ampliar la cantidad de dispositivos físicos, el responsable del área debe solicitar a través del "Software de Gestión de Incidentes" indicando la necesidad a la Sub Gerencia de Operaciones Telemáticas, para la evaluación y disponibilidad del servicio. La ampliación del número de dispositivos virtuales está reservada para los servidores civiles de la GTI.

7.3.1.6 El acceso remoto a los servicios de la red del RENIEC está permitido mediante una Red Privada Virtual (VPN - Virtual Private Network), gestionada desde la solución de Seguridad Perimetral, en la cual los datos y la información viajan sobre canales de acceso cifrados. El acceso remoto se autoriza por un tiempo determinado y, exclusivamente, para labores de administración de sistemas, aplicaciones y servicios críticos de la institución; de acuerdo a la DI-327-GTI/021 "Servicio de Comunicación para Usuarios Finales" numeral 6.8.

7.3.1.7 La computadora personal debe ser bloqueada por el usuario que la utiliza, cuando este se ausente de su puesto de trabajo, presionando simultáneamente las teclas "Control", "Alt" y "Supr" (o "Del" en algunos casos) y luego seleccionar la opción "Bloquear Computador"; para evitar el uso no autorizado del equipo y de las aplicaciones instaladas. El usuario que incumpla lo señalado es responsable por el uso no autorizado del equipo, de la red o de las aplicaciones instaladas.

7.3.1.8 A través de la red del RENIEC está prohibido almacenar y compartir archivos de música y video, ajenos a las actividades laborales y funciones asignadas a los usuarios. La Sub Gerencia de Operaciones Telemáticas está facultada a tomar las medidas preventivas necesarias para garantizar el rendimiento de la red.

7.3.1.9 El acceso a los servicios de RED para estaciones de trabajo alquiladas temporalmente a terceros, se otorga cumpliendo los siguientes lineamientos:

a. **Estaciones de trabajo nuevas**: Entregar junto con el equipo la media incluyendo la licencia de los productos adicionales preinstalados. La Sub Gerencia de Soporte Técnico Operativo verifica el estado del sistema operativo preinstalado y determina si requiere reinstalarse, para

posteriormente proceder a instalar las actualizaciones de seguridad.

b. **Estaciones de trabajo usadas**: Cuando esté disponible, entregar la media incluyendo la licencia de los productos adicionales preinstalados. La Sub Gerencia de Soporte Técnico Operativo verifica el estado del sistema operativo y lo reinstala en caso sea necesario, utilizando la media entregada. Si la media no está disponible, se debe proceder con la reconfiguración del equipo a los valores de fábrica.

c. En ambos casos es responsabilidad de la Sub Gerencia de Operaciones Telemáticas instalar el agente antivirus institucional y de la Sub Gerencia de Soporte Técnico Operativo la incorporación al dominio las estaciones de trabajo.

7.3.2 DE LA SEGURIDAD DE LOS DATOS

7.3.2.1 Para garantizar la confidencialidad se aplica un sistema de autenticación de usuarios registrados en una base de datos al cual se aplican las siguientes medidas de protección:

a. Contraseñas no menores de 8 caracteres.

b. Contraseñas encriptadas.

c. Formato y sintaxis de la contraseña predefinidos.

d. Periodo de expiración de sesión.

e. Tiempo de caducidad de contraseñas.

f. Acceso de las cuentas por roles predefinidos.

7.3.2.2 Para preservar la integridad de la información, se han implementado accesos vía certificados digitales y políticas de acceso a las bases de datos de acuerdo a la documentación interna de la institución.

7.3.2.3 Para garantizar la disponibilidad de los archivos que se encuentran en los servidores de base de datos y de aplicaciones y medios de comunicación, etc., están protegidos por mecanismos de seguridad para el acceso.

7.3.2.4 Los sistemas de comunicación poseen enlaces de respaldo y nivel de confiabilidad establecidos por la Subgerencia de Operaciones Telemáticas, complementándose con la inclusión de equipos de autonomía eléctrica (UPS´s y generadores eléctricos), tanto en equipos de comunicaciones, como en los servidores.

7.3.2.5 El acceso a los servidores y PC's solo se realiza mediante la autenticación.

7.3.2.6 En relación al no repudio de la información, se tiene mecanismos que permiten identificar el origen y recepción de la información.

7.3.2.7 Los equipos portátiles institucionales (Laptops) que son utilizados fuera de la red, deben utilizarse bajo las siguientes consideraciones:

a. La Sub Gerencia de Soporte Técnico Operativo crea cuentas locales personalizadas sin privilegios de administrador local.

b. Los discos duros deben estar cifrados, de acuerdo a la DI-354-GTI/003 "Uso de Dispositivos Móviles en el RENIEC" dispositivos móviles numeral 6.4.

7.4 DE LAS CONTRASEÑAS Y SEGURIDAD

7.4.1 Como parte de la política de seguridad de RENIEC, el sistema de seguridad solicita automáticamente al usuario el cambio de contraseña cada **45 días**. Se debe cambiar las contraseñas siempre que el usuario sospeche que la seguridad de su contraseña puede estar comprometida o vulnerada e informar a la Sub Gerencia de Operaciones Telemáticas para la evaluación correspondiente.

7.4.2 El formato y sintaxis de cada contraseña queda establecido bajo los siguientes lineamientos de formato, tamaño, número de caracteres y tiempo de vida:

a. Longitud mínima de 8 caracteres.

b. Combinación mínima obligatoria de letras mayúsculas, letras minúsculas, números y/o caracteres especiales.

c. Vigencia de **45 días**, al término de los cuales se fuerza el cambio de contraseña, no debe repetirse las tres últimas contraseñas.

7.4.3 Las contraseñas no deben ser enviadas en mensajes de correo electrónico, ni en ningún otro medio de comunicación electrónica. Tampoco deben ser reveladas o escritas en notas, documentos u otros medios escritos, incluyendo conversaciones telefónicas. Es responsabilidad directa de cada usuario mantener la contraseña en secreto y de uso personal exclusivo. Se exceptúa de este control al servicio VPN por no contar con un sistema de interacción directa con el usuario final para cambio de su contraseña.

7.4.4 Las contraseñas no deben ser palabras comunes o simples variaciones del nombre del servidor civil, usuario, nombre de la computadora, servidor o de la entidad. Por ejemplo, una contraseña fuerte puede ser; W94IjUp#2x4.

7.4.5 Durante el proceso de autenticación ante el sistema, el usuario tiene tres intentos para ingresar su contraseña correcta. Si en los tres intentos ingresa una contraseña incorrecta, la cuenta se bloquea automáticamente. Para activar nuevamente la cuenta debe enviar un correo electrónico a mesa de ayuda o a través del "Software de Gestión de Incidentes".

7.4.6 En las agencias que se conectan mediante accesos remotos a la red, a través de internet, el usuario debe realizar doble autenticación:

1. Para establecer el enlace privado con RENIEC.
2. Posteriormente, se autentica como usuario autorizado de un sistema en particular.

7.4.7 Ante situaciones de sustracción o pérdida de información del equipo de un usuario, causados por la violación de la cuenta, debido a una pobre definición o un mal uso de la contraseña, el usuario es responsable por los daños que pueda causar a los recursos informáticos del RENIEC, los cuales son evaluados por la Sub Gerencia de Operaciones Telemáticas y comunicado a la Gerencia de Talento Humano para su evaluación y acciones pertinentes.

7.5 DE LA GESTIÓN DE CUENTAS Y CLAVES DE SÚPER USUARIO

7.5.1 DE LA GESTIÓN DE CUENTAS DE SÚPER USUARIO PARA SERVIDORES, EQUIPOS DE RED Y SEGURIDAD

7.5.1.1 Los administradores de los servidores, equipos de red y seguridad usan herramientas especializadas de gestión de cuentas de súper usuario, donde se crean, modifican y resguardan las credenciales privilegiadas de los diferentes sistemas de información.

7.5.1.2 Los permisos de acceso expiran al año, en el caso que se supere los tres intentos fallidos en el proceso de autenticación de la cuenta estos son bloqueados automáticamente.

7.5.1.3 Las contraseñas de súper usuario deben contar como mínimo con las siguientes características:

a. Expiran una vez al año.

b. Longitud de 12 caracteres como mínimo.

c. Al menos un dígito alfanumérico.

d. No debe incluir tres caracteres iguales consecutivos.

e. Controlar el histórico de tres contraseñas.

7.5.2 DE LA GESTIÓN DE CUENTAS DE SÚPER USUARIO PARA ESTACIONES DE TRABAJO

7.5.2.1 El personal de la Sub Gerencia de Soporte Técnico Operativo incorpora por primera vez la estación de trabajo al Directorio Activo haciendo uso del súper usuario correspondiente; una vez concluida la actividad, la contraseña del súper usuario debe ser modificada en primera instancia por el personal de soporte técnico y posteriormente por la Sub Gerencia de Operaciones Telemáticas.

7.5.2.2 Las contraseñas del súper usuario de las estaciones de trabajo, son modificadas periódicamente por los administradores de la infraestructura del Directorio Activo.

7.5.2.3 Los asistentes informáticos de la Sub Gerencia de Soporte Técnico Operativo son los encargados de configurar la cuenta del usuario final, utilizando para ello el súper usuario o usuario administrador de aquellas estaciones de trabajo en se encuentran conectadas mediante el servicio VPN; una vez creado el usuario local, la contraseña del súper usuario debe ser modificada por otra predefinida por la Sub Gerencia de Operaciones Telemáticas.

7.5.3 DEL RESGUARDO DE CLAVES DE LAS CUENTAS DE SÚPER USUARIO

7.5.3.1 Los Sub Gerentes de Soporte Técnico Operativo y de Operaciones Telemáticas, tienen en custodia las cuentas de súper usuario en sobres lacrados para casos de contingencia, el sobre debe indicar:

a. Sistema o Plataforma Tecnológica asociada.

b. Fecha de expiración.

c. Fecha del último cambio.

7.5.4 DE LA CONTINGENCIA EN LA GESTIÓN DE CUENTAS DE SÚPER USUARIO

7.5.4.1 Los administradores de servidores, equipos de red y seguridad en caso de contingencia deben registrar las acciones de creación, modificación y/o eliminación de las cuentas de súper usuario, indicando lo siguiente:

a. Plataforma Tecnológica o Sistema de Información asociado.

b. Fecha y hora de la acción.

c. Acción realizada (creación, modificación y/o eliminación).

d. Autorización de la acción.

e. Nombre del usuario.

f. Cuenta de usuario relacionada.

g. Privilegios asignados.

7.5.4.2 Una vez superada la contingencia los Sub Gerentes de Soporte Técnico Operativo y de Operaciones Telemáticas coordinan con el Oficial de Seguridad de la información y los administradores de los sistemas de información los cambios que correspondan para el resguardo en un nuevo sobre sellado y la destrucción del sobre anterior.

7.6 DE LA PROTECCIÓN CONTRA ATAQUES INFORMÁTICOS, VIRUS, SOFTWARE MALICIOSO Y SIMILARES

7.6.1 DE LA PROTECCIÓN CONTRA ATAQUES INFORMÁTICOS

7.6.1.1 La Sub Gerencia de Operaciones Telemáticas controla los ataques informáticos mediante soluciones de seguridad de alto rendimiento y en alta disponibilidad.

7.6.1.2 El AntiDDoS, detecta y previene los ataques de denegación de servicio distribuido proveniente de la red pública de internet dirigido hacia nuestros servidores y servicios publicados.

7.6.1.3 Los Firewalls de Siguiente Generación, restringen los accesos externos a los servicios y aplicaciones web que publica el RENIEC. Estos dispositivos aíslan la red interna de la red pública internet y crean zonas de seguridad, abren o cierran puertos de servicio, habilitan o bloquean hosts de

origen y destino, trasladan direcciones IP públicas a direcciones IP internas de la red del RENIEC y viceversa.

7.6.1.4 Los sistemas de prevención de intrusiones detectan y evitan el ingreso de tráfico malicioso e indeseado a la red proveniente de internet, protegen a la red de ataques de denegación de servicio y ataques a nivel de aplicación.

7.6.1.5 Las políticas de seguridad son gestionadas a través de servidores centralizados, con las cuales se administran las soluciones de seguridad implementadas. Se tiene servidores repositorios de logs, donde se registran los accesos y eventos que son generados por cada una de las soluciones de seguridad; estos registros de accesos y eventos son almacenados por un periodo de seis meses.

7.6.2 DE LA PROTECCIÓN CONTRA VIRUS Y MALWARE

7.6.2.1 La Sub Gerencia de Operaciones Telemáticas cuenta con una solución de seguridad del endpoint (estaciones de trabajo, servidores y dispositivos móviles) y con una solución de seguridad de correo institucional para mitigar los virus o malware en las estaciones finales, servidores y en el tráfico entrante de correo electrónico proveniente de internet.

7.6.2.2 Como medida de prevención contra infecciones de malware, fuga y pérdida de la información se restringe el uso de los medios extraíbles de almacenamiento USB, cámaras digitales, módems inalámbricos y unidades de almacenamiento CD/DVD (dispositivos móviles), para lo cual se definen las siguientes políticas:

a. Para aquellos usuarios que por la naturaleza de sus funciones requieran la habilitación de medios extraíbles de almacenamiento como son: cámaras digitales, módems inalámbricos y unidades de almacenamiento CD/DVD (dispositivos móviles); el Jefe responsable del área debe solicitar a través del "Software de Gestión de Incidentes" adjuntando el "Formato de Habilitación de Medios Extraíbles de Almacenamiento" - Anexo N° 01 firmado digitalmente por el Gerente de la Unidad Orgánica y Jefe Regional y/o Jefes de Oficinas Registrales correspondiente, justificando la necesidad, adicionalmente debe adjuntar el "Acta de Confidencialidad para uso de Medios Extraíbles de Almacenamiento" firmado por el usuario final. Se exceptúa de esta disposición a los funcionarios con niveles de Gerente, Jefe de Oficina, Sub Gerente y Jefe Regional. Adicionalmente debe adjuntar el "Acta de Confidencialidad para Medios Extraíbles de Almacenamiento" firmado por el usuario final.

b. Por medidas de seguridad, se encuentra restringido el puerto USB a los servidores civiles. En caso se requiera para cumplimiento de sus funciones, el Gerente de la unidad orgánica correspondiente debe solicitar el acceso a través de un correo electrónico a la Sub Gerencia de Operaciones Telemáticas indicando las horas de acceso

que necesiten; el requerimiento es derivado al especialista de seguridad informática para su atención.

Una vez que se cumpla con el tiempo solicitado, el cual no debe exceder de ocho horas, se restringe nuevamente el acceso al puerto USB.

c. Cuando se detecte una infección o ataque en progreso, originado por el uso del medio extraíble de almacenamiento, el usuario es responsable por los daños de software y/o hardware causados por la infección; en este caso se revoca el permiso correspondiente.

7.6.2.3 La solución de seguridad del correo electrónico institucional, impide la propagación de mensajes maliciosos al servidor de correo del RENIEC y controla el ingreso de mensajes de correo provenientes de servidores gratuitos, analiza los archivos adjuntos, mitigando el riesgo de infección por virus y/o malware y cuenta con las siguientes políticas de seguridad:

a. Bloquear los mensajes provenientes de servidores de correo gratuito (hotmail, gmail, yahoo, etc.). Las excepciones para aquellos usuarios que por la naturaleza de sus funciones lo requieran deben solicitarse de acuerdo a la DI-327-GTI/021 "Servicio de Comunicación para Usuarios Finales" numeral 6.2.13.

b. Filtrar los mensajes entrantes que contienen archivos adjuntos de los siguientes tipos: ejecutables (*.exe, *.msi, etc.), comprimidos (*.zip,*.rar, etc), de música y video en todos sus formatos (*.mp3, *.wav, etc), entre otros; para prevenir el ingreso de contenido malicioso.

c. Evitar la usurpación de identidad, impidiendo el ingreso de mensajes provenientes de internet de supuestos remitentes que pertenecen al dominio "reniec.gob.pe".

d. Bloquear mensajes de correo que contiene publicidad, cadenas de mensajes, links para compras en red, listas de distribución, correo profano, contenido para adultos, phishing y otros.

e. Filtrar mensajes de correo que contengan frases claves de propósito malicioso e ingeniería social.

f. Crear listas blancas (remitentes permitidos) y listas negras (remitentes prohibidos).

7.6.2.4 El RENIEC tiene implementada la solución de Filtro de Contenido web, que restringe la navegación por páginas web prohibidas y mitiga la infección por descarga de archivos y software de internet, de acuerdo a la DI-327-GTI/021 "Servicio de Comunicación para Usuarios Finales" numeral 6.4.

7.6.2.5 Los archivos y/o programas de tipo ejecutables (*.exe, *.msi, etc.), comprimidos (*.zip,*.rar, etc.), música y video (*.mp3, *.wav, etc), entre otros, provenientes de fuentes no confiables de internet, pueden contener malware en

general; por ese motivo, su descarga en la red institucional está restringida.

En caso se requiera descargar algún programa desde internet se debe solicitar a la Sub Gerencia de Soporte Técnico Operativo, a través del "Software de Gestión de Incidentes", la instalación respectiva especificando el motivo de la necesidad y en que computadora(s) deben ser instalado(s). Previa evaluación de riesgos, el requerimiento es atendido. Se exceptúa de esta disposición al personal de la GTI, pues dentro de sus actividades se encuentra la verificación del impacto de la instalación de ciertos programas informáticos dentro de la red institucional.

7.6.2.6 Si en un computador se detecta una infección o malware en progreso o propagación, el analista y/o especialista de seguridad informática de la Sub Gerencia de Operaciones Telemáticas está facultado a tomar el control físico o remoto del equipo en cuestión a fin de controlar y mitigar los efectos del malware.

7.7 DE LA SEGURIDAD EN LA TRANSMISIÓN DE DATOS Y DOCUMENTOS ELECTRÓNICOS

7.7.1 La transmisión de datos, archivos y documentos electrónicos está garantizada por las medidas de seguridad propias de la gestión de la seguridad de la red que se indica en la presente directiva, la transmisión se realiza a través de la red privada y red pública.

a. **En la red privada** se transmiten datos, archivos y documentos electrónicos a los servidores de aplicaciones, servidores de bases de datos, servidores de almacenamiento y las estaciones de trabajo de las diferentes líneas de producción del RENIEC.

b. **En la red pública** se transmiten los servicios de consultas de datos que brinda RENIEC únicamente a instituciones que cuenten con direccionamiento IP público con origen en Perú, a excepción de los Consulados del Perú.

7.7.2 La transmisión libre de interceptaciones entre las estaciones emisoras y receptoras está garantizada por el uso de Certificados Digitales, Control de Accesos, Políticas de Grupo y Perfiles de Usuario, entre otros mecanismos contemplados en la presente Directiva.

7.7.3 Para las operaciones de transferencias de los registros electrónicos, archivos, datos automáticamente el sistema genera (log files), donde se encuentran registrados la fecha y hora de transferencia.

7.8 DEL USO DE LA CRIPTOGRAFIA

7.8.1 DE LA POLÍTICA SOBRE EL USO DE LA CRIPTOGRAFÍA

7.8.1.1 Se usan algoritmos criptográficos de cifrado fuerte en el aseguramiento de la información según corresponda, de acuerdo a la evaluación de riesgos.

7.8.1.2 Se utiliza la criptografía en los siguientes casos:

a. En la conexión segura a través del servicio VPN (Red Privada Virtual), por la red pública internet usando el

protocolo IPSec, de los locales remotos sin enlace de comunicación con el Centro de Datos.

b. En la transmisión de datos a través de enlaces dedicados a nivel nacional con el Centro de Datos, habilitando los mecanismos de encriptación/cifrado en los equipos routers remotos y en la cabecera del Centro de Datos.

c. En el cifrado de la información crítica del RENIEC.

d. En el cifrado de los discos duros de los dispositivos móviles (Laptop) del RENIEC.

e. En el envío de correo electrónico con información confidencial.

7.8.2 DE LA GESTIÓN DE CLAVES CRIPTOGRÁFICAS

7.8.2.1 Las claves criptográficas se mantienen en un equipamiento criptográfico externo mientras se utilizan o almacenan, con las medidas de seguridad adecuadas y se recuperan cuando los procesos lo requieran.

7.8.2.2 La Gerencia de Registros de Certificación Digital cumple con las disposiciones señaladas en la Guía de Acreditación para Entidades de Certificación (EC) aprobada por INDECOPI.

7.9 DE LAS VULNERABILIDADES TÉCNICAS

7.9.1 DE LA EVALUACIÓN DE LOS SERVIDORES DE APLICACIONES

7.9.1.1 La Sub Gerencia de Operaciones Telemáticas ejecuta el análisis de vulnerabilidades a todos los servidores y emite un reporte con las recomendaciones correspondientes a la Sub Gerencia de Ingeniería de Software o de Soporte Técnico Operativo, según sea el caso, para su corrección. Las referidas Sub Gerencias deben elaborar un plan de acción para mitigar los riesgos identificados.

7.9.2 DE LA EVALUACIÓN DE LOS SISTEMAS OPERATIVOS

7.9.2.1 La Sub Gerencia de Operaciones Telemáticas ejecuta el análisis de vulnerabilidades a los sistemas operativos de las estaciones de trabajo y servidores, dos veces al año, emitiendo un reporte con las vulnerabilidades encontradas para su corrección.

7.9.2.2 La Sub Gerencia de Operaciones Telemáticas planifica la instalación de los parches de seguridad correspondientes.

7.9.3 DE LA EVALUACIÓN DEL CÓDIGO DE DESARROLLO DE SOFTWARE

7.9.3.1 La Sub Gerencia de Ingeniería de Software durante el desarrollo de software debe basarse en el "Estándar para la Construcción Segura de Aplicaciones Web".

7.9.3.2 La Sub Gerencia de Operaciones Telemáticas realiza el análisis de vulnerabilidades de acuerdo a la DI-327-GTI/021 "Servicio de Comunicación para Usuarios Finales", numeral 7.9.1.

7.9.4 DE LA CORRECCIÓN DE LAS VULNERABILIDADES

7.9.4.1 Para la corrección de las vulnerabilidades encontradas, las Sub Gerencias de Ingeniería de Software, Soporte Técnico Operativo, Gestión de Bases de Datos y Operaciones Telemáticas ejecutan el plan para corregir las vulnerabilidades según corresponda.

7.9.4.2 La Sub Gerencia de Ingeniería de Software realiza las modificaciones que correspondan en el código del software evaluado.

7.9.4.3 La Sub Gerencia de Operaciones Telemáticas ejecuta un nuevo análisis de vulnerabilidades para verificar su corrección.

VIII. DISPOSICIONES COMPLEMENTARIAS

8.1 La Gerencia de Tecnología de la Información, a través de la Sub Gerencia de Operaciones Telemáticas, en coordinación con la Escuela Registral, promueven y organizan talleres de capacitación, a fin de garantizar el adecuado entendimiento, interpretación y aplicación de la presente directiva a todas las áreas del RENIEC.

IX. VIGENCIA

La presente directiva entra en vigencia a partir de su aprobación.

X. APROBACIÓN

Se aprueba mediante Resolución Secretarial.

XI. ANEXOS

ANEXO Nº 01

FORMATO DE HABILITACIÓN DE MEDIOS EXTRAIBLES DE ALMACENAMIENTO

FORMATO DE HABILITACIÓN DE MEDIOS EXTRAIBLES DE ALMACENAMIENTO

RENIEC — REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

DATOS DEL FORMATO: CÓDIGO: GC-7.F-HPUSB-08/SGOT-GTI/RE Versión: 02 Fecha Emisión: 28/07/2015 Fecha Actualización: 01/08/2017

N° Formato: 00001/SGPP/GII FECHA DE SOLICITUD: 01/02/2017

DATOS DEL SOLICITANTE			
GERENCIA/OFICINA:	Gerencia de Imagen Institucional		
SUB GERENCIA/JEFATURA REGIONAL/ JEFE DE OFICINA REGISTRAL:	Sub Gerencia de Relaciones Públicas		
NOMBRES Y APELLIDOS:	Diana Mora		
DATOS DEL CONTACTO:			
Nombres y Apellidos:	Nelly Portocarrero	Teléfono de contacto:	1151
DATOS DEL SERVIDOR CIVIL/ LOCADOR DE SERVICIOS:			
Nombres y Apellidos:	Sandra Rivas	Turno:	Mañana
Unidad Orgánica:	GII/SGPP		
Ubicación:	Sede Administrativa Piso: 29	Dirección:	Jr. Bolivia N° 109
Tipo de Solicitud:	Habilitación [X]	Bloqueo	[ ]

DATOS DEL REQUERIMIENTO

Tipo de Solicitud: Habilitación

		Equipo / IP	Marca	Modelo
a) Cámaras Digitales	[X]			
b) Modems Inalámbricos	[ ]			
c) Unidades de almacenamiento (CDs y DVDs)	[ ]			

Justificación:

GERENCIA PLANIFICACIÓN Y PRESUPUESTO

GERENCIA TECNOLOGÍAS DE LA INFORMACIÓN

SUB GERENCIA DE ASESORÍA ADMINISTRATIVA

GERENCIA ASESORÍA JURÍDICA

ANEXO N° 02

ACTA DE CONFIDENCIALIDAD PARA MEDIOS EXTRAIBLES DE ALMACENAMIENTO

Yo, ... con DNI N°..... servidor civil de la Gerencia / Oficina / Sub Gerencia /Jefatura Regional de ....., me comprometo a cumplir con los siguientes puntos:

- La información del RENIEC que por razones de trabajo copie al Medio Extraíble de Almacenamiento, solo lo utilizaré dentro de la institución y para el cumplimiento de las labores encomendadas.
- Mantener la ***confidencialidad y privacidad*** de la información del RENIEC al que tengo acceso.
- Cumplir con lo estipulado en la Directiva DI-328-GTI/022 "Seguridad Informática de la Red del RENIEC".

En caso de incumplimiento, me acojo a lo establecido a las normas laborales, así como la Ley del Procedimiento Administrativo General (Ley N° 27444).

Firma

Lima, ... de .....de 20.....

ANEXO N° 03
CUADRO DE CONTROL DE CAMBIOS

"SEGURIDAD INFORMÁTICA DEL RENIEC"	
IDENTIFICACIÓN DEL CAMBIO	
NUMERAL VIGENTE	**NUMERAL MODIFICADO**
II. ALCANCE	**II. ALCANCE**
III. BASE LEGAL	**III. BASE LEGAL**
Numeral 3.2	Eliminado
Numeral 3.3	Numeral 3.2
Numeral 3.4	Numeral 3.3
Numeral 3.5	Numeral 3.4
Numeral 3.6	Numeral 3.5
No existía en esta versión	Numeral 3.6
Numeral 3.9	Eliminado
Numeral 3.10	Numeral 3.9
No existía en esta versión	Numeral 3.10
Numeral 3.14	Eliminado
Numeral 3.15	Numeral 3.14
Numeral 3.16	Numeral 3.15
No existía en esta versión	Numeral 3.16
Numeral 3.17	Numeral 3.17
IV. DEFINICIÓN DE TERMINOS	**IV. DEFINICIÓN DE TERMINOS**
No existía en esta versión	Numeral 4.1
Numeral 4.1	Numeral 4.2
No existía en esta versión	Numeral 4.3
Numeral 4.2	Numeral 4.4
No existía en esta versión	Numeral 4.5
No existía en esta versión	Numeral 4.6
Numeral 4.3	Numeral 4.7
No existía en esta versión	Numeral 4.8
No existía en esta versión	Numeral 4.9
No existía en esta versión	Numeral 4.10
No existía en esta versión	Numeral 4.11
Numeral 4.4	Numeral 4.12
Numeral 4.5	Numeral 4.13
No existía en esta versión	Numeral 4.14
No existía en esta versión	Numeral 4.15
No existía en esta versión	Numeral 4.16
No existía en esta versión	Numeral 4.17
Numeral 4.6	Numeral 4.18
No existía en esta versión	Numeral 4.19
Numeral 4.7	Numeral 4.20
Numeral 4.8	Numeral 4.21
Numeral 4.9	Numeral 4.22
No existía en esta versión	Numeral 4.23
No existía en esta versión	Numeral 4.24
Numeral 4.10	Eliminado
No existía en esta versión	Numeral 4.25
Numeral 4.11	Numeral 4.26

"SEGURIDAD INFORMÁTICA DEL RENIEC"	
IDENTIFICACIÓN DEL CAMBIO	
NUMERAL VIGENTE	**NUMERAL MODIFICADO**
Numeral 4.12	Numeral 4.27
No existía en esta versión	Numeral 4.28
Numeral 4.13	Numeral 4.29
Numeral 4.14	Numeral 4.30
Numeral 4.15	Numeral 4.31
No existía en esta versión	Numeral 4.32
Numeral 4.16	Numeral 4.33
Numeral 4.17	Eliminado.
Numeral 4.18	Numeral 4.34
Numeral 4.19	Eliminado.
Numeral 4.20	Numeral 4.35
Numeral 4.21	Eliminado
No existía en esta versión	Numeral 4.36
Numeral 4.22	Numeral 4.37
V. RESPONSABILIDADES	**V.RESPONSABILIDADES**
Numeral 5.1	Numeral 5.1
Numeral 5.2	Numeral 5.2
Numeral 5.3	Numeral 5.3
Numeral 5.4	Numeral 5.3
No existe en esta versión	Numeral 5.4
Numeral 5.6	Numeral 5.6
Numeral 5.7	Numeral 5.7
Numeral 5.8	Numeral 5.8
No existe en esta versión	Numeral 5.9
No existe en esta versión	Numeral 5.10
VI. DISPOSICIONES GENERALES	**VI. DISPOSICIONES GENERALES**
6.1 DE LA SEGURIDAD DE LOS RECURSOS INFORMÁTICOS	**6.1 DE LA SEGURIDAD DE LOS RECURSOS INFORMÁTICOS**
Numeral 6.1.1	Numeral 6.1.1
Numeral 6.1.2	Numeral 6.1.2
6.2 DE LA SEGURIDAD FÍSICA Y DEL ENTORNO	**6.2 DE LA SEGURIDAD FÍSICA Y DEL ENTORNO**
Numeral 6.2.1	Numeral 6.2.1
Numeral 6.2.3	Eliminado.
Numeral 6.2.4	Numeral 6.2.3
6.3 DEL CONTROL DE ACCESO A LA RED, SUS SERVICIOS, AL SISTEMA OPERATIVO Y SEGURIDAD DE LOS DATOS	**6.3 DEL CONTROL DE ACCESO A LA RED Y SEGURIDAD DE LOS DATOS**
Numeral 6.3.4	Numeral 6.3.4
Numeral 6.3.5	Numeral 6.3.5
Numeral 6.3.7	Numeral 6.3.7
Numeral 6.3.8	Numeral 6.3.8
Numeral 6.3.9	Numeral 6.3.9
6.4 DE LAS CONTRASEÑAS Y SEGURIDAD	**6.4 DE LAS CONTRASEÑAS Y SEGURIDAD**
Numeral 6.4.1	Numeral 6.4.1

"SEGURIDAD INFORMÁTICA DEL RENIEC"	
IDENTIFICACIÓN DEL CAMBIO	
NUMERAL VIGENTE	**NUMERAL MODIFICADO**
Numeral 6.4.2	Numeral 6.4.2
No existía en esta versión	Numeral 6.4.3
6.5 DE LA GESTION DE CUENTAS Y CLAVES DE SÚPER USUARIO	**6.5 DE LA GESTION DE CUENTAS Y CLAVES DE SÚPER USUARIO**
Numeral 6.5.1	Numeral 6.5.1
Numeral 6.5.2	Numeral 6.5.2
6.6 DE LA PROTECCIÓN CONTRA ATAQUES INFORMÁTICOS, VIRUS, SOFTWARE MALICIOSO Y SIMILARES	**6.6 DE LA PROTECCIÓN CONTRA ATAQUES INFORMÁTICOS, VIRUS, SOFTWARE MALICIOSO Y SIMILARES**
Numeral 6.6.1	Numeral 6.6.1
Numeral 6.6.2	Numeral 6.6.2
6.7 DE LA SEGURIDAD EN LA TRANSMISIÓN DE DATOS Y DOCUMENTOS ELECTRÓNICOS	**6.7 DE LA SEGURIDAD EN LA TRANSMISIÓN DE DATOS Y DOCUMENTOS ELECTRÓNICOS**
Numeral 6.7.1	Numeral 6.7.1
No existía en esta versión	**6.8 DEL USO DE LOS CONTROLES CRIPTOGRÁFICOS**
No existía en esta versión	Numeral 6.8.1
No existía en esta versión	Numeral 6.8.2
No existía en esta versión	**6.9 DE LAS VULNERABILIDADES TECNICAS**
No existía en esta versión	Numeral 6.9.1
No existía en esta versión	Numeral 6.9.2
No existía en esta versión	Numeral 6.9.3
VII. DISPOSICIONES ESPECIFICAS	**VII. DISPOSICIONES ESPECÍFICAS**
7.1 DE LA SEGURIDAD DE LOS RECURSOS INFORMÁTICOS	**7.1 DE LA SEGURIDAD DE LOS RECURSOS INFORMÁTICOS**
No existía en esta versión	**7.1.1 ÁREAS SEGURAS**
Numeral 7.1.1	Numeral 7.1.1.1
Numeral 7.1.2	Numeral 7.1.1.2
Numeral 7.1.3	Numeral 7.1.1.3
Numeral 7.1.4	Eliminado.
Numeral 7.1.5	Numeral 7.1.1.4
Numeral 7.1.5.1	Numeral 7.1.1.5
Numeral 7.1.5.2	Numeral 7.1.1.6
Numeral 7.1.5.3	Eliminado
7.2 DE LA SEGURIDAD FÍSICA Y DEL ENTORNO	**7.2 DE LA SEGURIDAD FÍSICA Y DEL ENTORNO**
7.2.1 DE LAS ESTACIONES DE TRABAJO	**7.2.1 DE LAS ESTACIONES DE TRABAJO**
Numeral 7.2.1.1	Numeral 7.2.1.1
Numeral 7.2.1.1	Numeral 7.2.1.2
Numeral 7.2.1.2	Numeral 7.2.1.3
7.2.2 DE LOS EQUIPOS DE	**7.2.2 DE LOS EQUIPOS DE**

"SEGURIDAD INFORMÁTICA DEL RENIEC"	
IDENTIFICACIÓN DEL CAMBIO	
NUMERAL VIGENTE	**NUMERAL MODIFICADO**
COMUNICACIÓN QUE SE UBICAN EN EL CENTRO DE CÓMPUTO	**COMUNICACIÓN QUE SE UBICAN EN EL CENTRO DE CÓMPUTO**
Numeral 7.2.2.1	Numeral 7.2.2.1
Numeral 7.2.2.2	Numeral 7.2.2.2
Numeral 7.2.2.3	Numeral 7.2.2.3
7.2.3 DE LOS EQUIPOS DE COMUNICACIONES INSTALADOS EN LOS RACKS DE COMUNICACIONES DE CADA PISO EN SEDES Y OFICINAS REGISTRALES	**7.2.3 DE LOS EQUIPOS DE COMUNICACIONES INSTALADOS EN LOS RACKS DE COMUNICACIONES DE CADA PISO EN SEDES Y OFICINAS REGISTRALES**
Numeral 7.2.3.1	Numeral 7.2.3.1
Numeral 7.2.3.2	Numeral 7.2.3.2
Numeral 7.2.3.3	Numeral 7.2.3.3
Numeral 7.2.3.4	Eliminado.
7.3 DEL CONTROL DE ACCESO A LA RED, SUS SERVICIOS, AL SISTEMA OPERATIVO Y SEGURIDAD DE LOS DATOS	**7.3 DEL CONTROL DE ACCESO A LOS SERVICIOS DE RED Y SEGURIDAD DE LOS DATOS**
7.3.1 DEL CONTROL DE ACCESOS A LA RED	**7.3.1 DEL CONTROL DE ACCESOS A LOS SERVICIOS DE RED**
Numeral 7.3.1.1	Numeral 7.3.1.1
Numeral 7.3.1.2	Numeral 7.3.1.2
Numeral 7.3.1.3	Numeral 7.3.1.3
Numeral 7.3.1.4	Numeral 7.3.1.4
Numeral 7.3.1.5	Numeral 7.3.1.5
Numeral 7.3.1.6	Eliminado.
Numeral 7.3.1.7	Eliminado.
Numeral 7.3.1.8	Numeral 7.3.1.6
Numeral 7.3.1.9	Eliminado.
Numeral 7.3.1.10	Eliminado.
7.3.2 DEL CONTROL DE ACCESO AL SISTEMA OPERATIVO	Eliminado.
Numeral 7.3.2.1	Eliminado.
Numeral 7.3.2.2	Eliminado.
Numeral 7.3.2.3	Eliminado.
Numeral 7.3.2.4	Eliminado.
Numeral 7.3.2.5	Numeral 7.3.1.7
Numeral 7.3.2.6	Numeral 7.3.1.8
No existía en esta versión.	Numeral 7.3.1.9
7.3.3 DE LA SEGURIDAD DE LOS DATOS	**7.3.2 DE LA SEGURIDAD DE LOS DATOS**
Numeral 7.3.3.1	Numeral 7.3.2.1
Numeral 7.3.3.2	Numeral 7.3.2.2
Numeral 7.3.3.3	Numeral 7.3.2.3
Numeral 7.3.3.4	Numeral 7.3.2.4
Numeral 7.3.3.5	Numeral 7.3.2.5
Numeral 7.3.3.6	Numeral 7.3.2.6

"SEGURIDAD INFORMÁTICA DEL RENIEC"	
IDENTIFICACIÓN DEL CAMBIO	
NUMERAL VIGENTE	**NUMERAL MODIFICADO**
No existía en esta versión.	Numeral 7.3.2.7
7.4 DE LAS CONTRASEÑAS Y SEGURIDAD	**7.4 DE LAS CONTRASEÑAS Y SEGURIDAD**
Numeral 7.4.1	Numeral 7.4.1
Numeral 7.4.2	Numeral 7.4.2
Numeral 7.4.3	Numeral 7.4.3
Numeral 7.4.4	Numeral 7.4.4
Numeral 7.4.5	Numeral 7.4.5
Numeral 7.4.6	Numeral 7.4.6
Numeral 7.4.7	Numeral 7.4.7
7.5 DE LA GESTIÓN DE CUENTAS Y CLAVES DE SÚPER USUARIO	**7.5 DE LA GESTIÓN DE CUENTAS Y CLAVES DE SÚPER USUARIO**
7.5 1 DE LA ASIGNACIÓN DE CUENTAS DE SÚPER USUARIOS	Eliminado
Numeral 7.5.1.1	Eliminado
Numeral 7.5.1.2	Se encuentra en el numeral 7.5.4.1
No existía en esta versión.	**7.5 1 DE LA GESTION DE CUENTAS DE SÚPER USUARIO PARA SERVIDORES, EQUIPOS DE RED Y SEGURIDAD**
No existía en esta versión.	Numeral 7.5.1.1
Numeral 7.5.2.2	Numeral 7.5.1.2
Numeral 7.5.2.3	Numeral 7.5.1.3
No existía en esta versión.	**7.5 2 DE LA GESTIÓN DE CUENTAS DE SUPER USUARIO PARA ESTACIONES DE TRABAJO**
No existía en esta versión.	Numeral 7.5.2.1
No existía en esta versión.	Numeral 7.5.2.2
No existía en esta versión.	Numeral 7.5.2.3
7.5.2 DEL RESGUARDO DE CLAVES DE LAS CUENTAS DE SUPER USUARIO	**7.5 3 DEL RESGUARDO DE CLAVES DE LAS CUENTAS DE SUPER USUARIO**
Numeral 7.5.2.1	Numeral 7.5.3.1
Numeral 7.5.2.2	Se encuentra en el numeral 7.5.1.2.
Numeral 7.5.2.3	Se encuentra en el numeral 7.5.1.3.
7.5 3 DE LA CONTINGENCIA EN EL MANEJOS DE LAS CONTRASEÑAS DE CUENTAS DE SÚPER USUARIO	Eliminado.
Numeral 7.5.3.1	Eliminado.
Numeral 7.5.3.2	Eliminado.
No existía en esta versión.	**7.5 4 DE LA CONTINGENCIA EN LA GESTIÓN DE CUENTAS DE SÚPER USUARIO**
Numeral 7.5.1.2	Numeral 7.5.4.1
Numeral 7.5.3.3	Numeral 7.5.4.2
Numeral 7.5.3.4	Eliminado.
7.6 DE LA PROTECCIÓN	**7.6 DE LA PROTECCIÓN**

"SEGURIDAD INFORMÁTICA DEL RENIEC"	
IDENTIFICACIÓN DEL CAMBIO	
NUMERAL VIGENTE	**NUMERAL MODIFICADO**
CONTRA ATAQUES INFORMATICOS, VIRUS, SOFTWARE MALICIOSO Y SIMILARES	**CONTRA ATAQUES INFORMATICOS, VIRUS, SOFTWARE MALICIOSO Y SIMILARES**
7.6.1 DE LA PROTECCIÓN CONTRA ATAQUES INFORMÁTICOS	**7.6.1 DE LA PROTECCIÓN CONTRA ATAQUES INFORMÁTICOS**
Numeral 7.6.1.1	Numeral 7.6.1.1
No existía en esta versión.	Numeral 7.6.1.2
Numeral 7.6.1.2	Numeral 7.6.1.3
Numeral 7.6.1.3	Numeral 7.6.1.4
Numeral 7.6.1.4	Numeral 7.6.1.5
7.6.2 DE LA PROTECCIÓN CONTRA VIRUS Y MALWARE	**7.6.2 DE LA PROTECCIÓN CONTRA VIRUS Y MALWARE**
No existía en esta versión.	Numeral 7.6.2.1
Numeral 7.6.2.1	Numeral 7.6.2.2
Numeral 7.6.2.2	Eliminado
Numeral 7.6.2.3	Eliminado
Numeral 7.6.2.4	Numeral 7.6.2.3
Numeral 7.6.2.5	Numeral 7.6.2.3 literal a)
Numeral 7.6.2.6	Numeral 7.6.2.3 literal c)
Numeral 7.6.2.7	Numeral 7.6.2.4
Numeral 7.6.2.8	Numeral 7.6.2.4 literal f)
Numeral 7.6.2.9	Numeral 7.6.2.5
Numeral 7.6.2.10	Numeral 7.6.2.6
Numeral 7.6.2.11	Numeral 7.6.2.7
No existía en esta versión.	**7.8 DEL USO DE LA CRIPTOGRAFIA**
No existía en esta versión.	**7.8.1 DE LA POLÍTICA SOBRE EL USO DE LA CRIPTOGRAFÍA**
No existía en esta versión.	Numeral 7.8.1.1
No existía en esta versión.	Numeral 7.8.1.2
No existía en esta versión.	**7.8.2 DE LA GESTIÓN DE CLAVES CRIPTOGRAFIAS**
No existía en esta versión.	Numeral 7.8.2.1
No existía en esta versión.	Numeral 7.8.2.2
No existía en esta versión.	**7.9 DE LAS VULNERABILIDADES TÉCNICAS**
No existía en esta versión	**7.9.1 DE LA EVALUACIÓN DE LOS SERVIDORES DE APLICACIONES**
No existía en esta versión	Numeral 7.9.1.1
No existía en esta versión	**7.9.2 DE LA EVALUACIÓN DE LOS SISTEMAS OPERATIVOS**
No existía en esta versión	Numeral 7.9.2.1
No existía en esta versión	Numeral 7.9.2.2
No existía en esta versión	**7.9.3 DE LA EVALUACIÓN DEL CÓDIGO DE DESARROLLO DE SOFTWARE**

"SEGURIDAD INFORMÁTICA DEL RENIEC"	
IDENTIFICACIÓN DEL CAMBIO	
NUMERAL VIGENTE	**NUMERAL MODIFICADO**
No existía en esta versión	Numeral 7.9.3.1
No existía en esta versión	Numeral 7.9.3.2
No existía en esta versión	**7.9.4 DE LA CORRECIÓN DE LAS VULNERABILIDADES**
No existía en esta versión	Numeral 7.9.4.1
No existía en esta versión	Numeral 7.9.4.2
No existía en esta versión	Numeral 7.9.4.3
No existía en esta versión.	**VIII.DISPOSICIONES COMPLEMENTARIAS**
VIII. VIGENCIA	**IX. VIGENCIA**
IX. APROBACIÓN	**X.APROBACIÓN**
X. ANEXOS	**XI. ANEXOS**
Anexo N° 01	Anexo N° 01
Anexo N° 02	Anexo N° 02
Anexo N° 03	Anexo N° 03