DIRECTIVA

USO DE DISPOSITIVOS MÓVILES EN EL RENIEC

RESOLUCIÓN SECRETARIAL N° 96 -2018/SGEN/RENIEC		
DI-354-GTI/003	VERSIÓN: 03 N° PÁGINAS: 14	FECHA DE APROBACIÓN 10 JUL. 2018

INDICE

I. OBJETIVO 3
II. ALCANCE 3
III. BASE LEGAL 3
IV. DEFINICIÓN DE TERMINOS 4
V. RESPONSABILIDADES 5
VI. DISPOSICIONES GENERALES 6
VII. DISPOSICIONES ESPECÍFICAS 7
VIII. DISPOSICIONES COMPLEMENTARIAS 10
IX. VIGENCIA 10
X. APROBACIÓN 10
XI. ANEXO 10
ANEXO N° 01 11
FORMATO DE EVALUACIÓN DE DISPOSITIVOS MÓVILES EXTERNOS 11
ANEXO N° 02 12
CUADRO DE CONTROL DE CAMBIOS 12

I. OBJETIVO

Establecer lineamientos para normar y garantizar el uso adecuado de los Servicios de Telecomunicaciones del Registro Nacional de Identificación y Estado Civil – RENIEC mediante dispositivos móviles.

II. ALCANCE

La presente Directiva es administrada por la Gerencia de Tecnología de la Información (GTI), a través de la Sub Gerencia de Operaciones Telemáticas (SGOT) y es de aplicación obligatoria para todos los servidores civiles del RENIEC que hacen uso de los dispositivos móviles autorizados por el 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 y sus modificatorias.

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

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

3.5 **Decreto Supremo N° 072-2003-PCM,** aprueba el Reglamento de la Ley de Transparencia y Acceso a la Información Pública, del 07 de agosto de 2003.

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 de 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° 004-2016-PCM,** aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática, del 14 de Enero de 2016.

3.9 **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 20 de junio de 2017.

3.10 **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 de 2015.

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

3.12 **Resolución Jefatural N° 069-2017/JNAC/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.

3.13 **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 Confidencialidad

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

4.2 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.

4.3 Dispositivos Móviles

Son aparatos electrónicos de diversos tamaños, algunos de ellos con grandes capacidades de procesamiento, almacenamiento y memoria RAM; con conexión inalámbrica y/o alámbrica a una red, que han sido diseñados para múltiples funciones. Se incluyen en este tipo de dispositivos: Computadoras Portátiles, Teléfonos Inteligentes (smartphones), Tabletas (Tablets) o similares.

4.4 Dispositivos Móviles de Proveedores

Son aparatos electrónicos, tales como teléfonos inteligentes (smartphones), computadoras portátiles, tabletas y/o similares, pertenecientes a proveedores de bienes y/o servicios que cuentan con contrato vigente con el RENIEC.

4.5 Dispositivos Móviles de Administradores de Servicios Críticos

Son aparatos electrónicos, tales como teléfonos inteligentes (smartphones), computadoras portátiles, tabletas y/o similares, de propiedad del personal que labora en la Gerencia de Soporte Técnico Operativo y la Sub Gerencia de Operaciones Telemáticas del RENIEC y que a su vez es responsable por la administración de servicios informáticos de misión crítica (Datacenter, Servidores, Radioenlaces, Equipos de Comunicaciones y Seguridad Informática) y que utilizan estos dispositivos móviles para la administración/monitoreo de los servicios a su cargo.

4.6 Dispositivos Móviles de Visitantes

Son aparatos electrónicos, tales como teléfonos inteligentes (smartphones), computadoras portátiles, tabletas y/o similares, pertenecientes a terceros, que ingresan al RENIEC en calidad de visitantes y cuya visita no está relacionada a la prestación de algún servicio o solución de algún incidente.

4.7 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.´

4.8 **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.

4.9 **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.

4.10 **Seguridad Informática**

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

4.11 **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.

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 Es responsabilidad de la Oficina de Seguridad y Defensa Nacional – OSDN controlar el ingreso de los dispositivos móviles de los proveedores con contrato vigente con el RENIEC o de los visitantes, autorizados por el Gerente, Jefe de Oficina y Jefe del área usuaria según corresponda.

5.3 La Sub Gerencia de Operaciones Telemáticas es la responsable de la seguridad de las redes de comunicación y acceso a internet, así como asegurar la integridad de los datos durante su transmisión.

5.4 La Sub Gerencia de Operaciones Telemáticas, es responsable de definir, implementar, mantener y monitorear los controles de seguridad que correspondan aplicar a los dispositivos móviles.

5.5 La Sub Gerencia de Operaciones Telemáticas, es responsable de revisar los dispositivos móviles que van a acceder a la red del RENIEC y realizar el análisis de riesgo correspondiente.

5.6 La instalación y configuración de los servicios de comunicación en los dispositivos móviles, de propiedad del RENIEC, es responsabilidad de la Sub Gerencia de Operaciones Telemáticas; así como la instalación del antivirus institucional en los dispositivos, en caso sea necesario, y siempre y cuando los soporten.

5.7 Es responsabilidad de los funcionarios del RENIEC, reportar de forma inmediata en caso de robo o extravío de los dispositivos móviles a la Sub Gerencia de Operaciones Telemáticas para ejecutar las acciones correctivas y así resguardar la información institucional crítica que contiene el dispositivo.

VI. DISPOSICIONES GENERALES

6.1 La conexión a la red del RENIEC, para uso del servicio de internet, se permite a los dispositivos móviles de propiedad de la institución y del personal que administra servicios informáticos críticos (autorizados por su área), así como de los dispositivos móviles de los proveedores con contrato vigente (autorizados por el área correspondiente y controlados por la Oficina de Seguridad y Defensa Nacional – OSDN.

La Sub Gerencia de Operaciones Telemáticas antes de otorgar los accesos solicitados, revisa los dispositivos móviles y realiza el análisis de riesgo respectivo en el "Formato de Evaluación de Dispositivos Móviles Externos" - Anexo N° 01 y firma digitalmente.

6.2 DEL ACCESO A LA RED DEL RENIEC, DE LAS CONTRASEÑAS Y SEGURIDAD EN LOS DISPOSITIVOS MÓVILES DE PROPIEDAD DEL RENIEC

6.2.1 Los dispositivos móviles, tales como computadoras portátiles, teléfonos inteligentes (smartphones), tabletas o similares, de propiedad del RENIEC son protegidos por las soluciones de seguridad informática implementadas (administrados por la Sub Gerencia de Operaciones Telemáticas) y sujeto a todos los controles de seguridad establecidos, para garantizar que no se comprometa la información del RENIEC. Cualquier cambio en la configuración de algún equipo debe ser autorizado por la Sub Gerencia de Operaciones Telemáticas.

6.2.2 Los dispositivos móviles (laptops y tabletas con sistemas operativos Windows) de propiedad del RENIEC, se conectan a la red mediante el perfil de dominio asignado a los servidores civiles.

6.2.3 Los dispositivos móviles de propiedad del RENIEC cuentan con una contraseña de protección para acceso al dispositivo. Adicionalmente con un mecanismo de cifrado de contenido o similares para prevenir el acceso no autorizado a la información contenida en ellos.

6.2.4 Los servidores civiles deben mantener todas las configuraciones de seguridad establecidas en el dispositivo.

6.3 DE LA CONEXIÓN A LA RED DEL RENIEC DE DISPOSITIVOS MÓVILES DEL PERSONAL ADMINISTRADOR DE SERVICIOS CRÍTICOS

6.3.1 Con autorización de los Sub Gerentes de Soporte Técnico Operativo y de Operaciones Telemáticas se permite el acceso a la red del RENIEC a los dispositivos móviles de propiedad de los servidores civiles que son responsables de la administración de servicios informáticos de misión crítica (Datacenter, Servidores, Radioenlaces, Equipos de Comunicaciones y Seguridad Informática); que son utilizados para la administración/monitoreo de los servicios a su cargo.

6.4 DE LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES Y SU CONTENIDO FUERA DE LAS INSTALACIONES DEL RENIEC

6.4.1 Los dispositivos móviles de propiedad del RENIEC o de los servidores civiles que administran servicios informáticos de misión

crítica, que son usados en lugares públicos o privados y se conectan a una red inalámbrica o alámbrica que no es administrada por la Institución, es responsable de la seguridad física y de la información que comparta con terceros a través de esa red.

6.4.2 Los dispositivos móviles que se encuentren fuera de la red del RENIEC se conectan a la red a través del servicio VPN.

6.5 DE LA CONEXIÓN DE DISPOSITIVOS MÓVILES DE PROVEEDORES O VISITANTES A LA RED DEL RENIEC Y/O SU SERVICIO DE INTERNET

6.5.1 Cuando los proveedores, con contrato vigente, realicen labores de soporte, mantenimiento, implementación de soluciones, entre otros, cuyo ingreso a las instalaciones del RENIEC ha sido autorizado por el área responsable e inspeccionados por el personal de la Oficina de Seguridad y Defensa Nacional; se permite la conexión temporal a la red de sus equipos móviles.

El área correspondiente solicita el acceso a la red y de ser necesario el servicio de Internet a través del "Software de Gestión de Incidentes" de la Sub Gerencia de Soporte Técnico Operativo, sustentando el motivo e indicando los trabajos a realizar y el tiempo de permanencia del proveedor; previa evaluación de riesgos en el "Formato de Evaluación de Dispositivos Móviles Externos" - Anexo N° 01, la Sub Gerencia de Operaciones Telemáticas atiende la solicitud. Una vez brindado los permisos y accesos correspondientes el área solicitante es responsable del buen uso de los servicios otorgados a estos dispositivos.

6.5.2 Los equipos móviles de visitantes sin contrato con el RENIEC, cuyo ingreso a las instalaciones del RENIEC es autorizado por el área responsable y que fue inspeccionado por el personal de la Oficina de Seguridad y Defensa Nacional, y requieran del servicio de Internet temporal; debe ser solicitado por el área responsable por medio del "Software de Gestión de Incidentes" de la Sub Gerencia de Soporte Técnico Operativo, explicando el motivo de la solicitud e indicando el tiempo de permanencia del visitante, con un día de anticipación.

La Sub Gerencia de Operaciones Telemáticas atiende la solicitud, previa evaluación de riesgos en el "Formato de Evaluación de Dispositivos Móviles Externos" - Anexo N° 01, el área solicitante es responsable del buen uso del servicio otorgado a estos dispositivos.

6.5.3 No se permite la conexión a la red del RENIEC a los dispositivos móviles que no cumplen con los lineamientos y condiciones especificadas en el presente documento.

VII. DISPOSICIONES ESPECÍFICAS

7.1 DEL ACCESO A LA RED DEL RENIEC, DE LAS CONTRASEÑAS Y SEGURIDAD EN LOS DISPOSITIVOS MÓVILES DE PROPIEDAD DEL RENIEC

7.1.1. DEL ACCESO A LA RED DEL RENIEC

7.1.1.1 La configuración de todos los equipos móviles de propiedad del RENIEC para el acceso a la red se realiza de acuerdo a las políticas de seguridad establecidas en la presente directiva.

7.1.1.2 Para la conexión a la red inalámbrica de un dispositivo móvil de propiedad del RENIEC, éste debe contar con credenciales para autenticarse a la red. Las credenciales para un dispositivo móvil específico, debe ser solicitado a través del "Software de Gestión de Incidentes" a la Sub Gerencia de Soporte Técnico Operativo.

7.1.1.3 El usuario final debe contar con un perfil de dominio (en el caso de que el dispositivo móvil cuente con Sistema Operativo Windows) adicional a las credenciales, para acceder a la red del RENIEC. Los accesos a los diferentes recursos de la red son definidos de acuerdo al perfil del usuario de dominio correspondiente.

7.1.2 DE LAS CONTRASEÑAS Y SEGURIDAD EN LOS DISPOSITIVOS MÓVILES

7.1.2.1 Se asigna una contraseña para el acceso al dispositivo informático móvil de propiedad del RENIEC, tales como: Computadoras portátiles, teléfonos inteligentes (smartphones), tabletas o similares y se realiza todas las configuraciones necesarias como instalación de antivirus, actualización del Sistema Operativo y el cifrado de contenido, antes de ser entregado al usuario final.

7.1.2.2 Los teléfonos móviles - Smartphone que requieren cambio por desperfecto u otro motivo, se debe informar a la Sub Gerencia de Operaciones Telemáticas para que realice el proceso de reseteo a los valores de fábrica del dispositivo, siempre y cuando que el dispositivo guarde información confidencial del RENIEC o haya sido conectado a la red para consumir sus servicios.

7.1.2.3 Por sustracción o pérdida de los teléfonos móviles – Smartphone, el Funcionario del RENIEC debe comunicar en el acto a:

a. La Sub Gerencia de Operaciones Telemáticas para la activación de las políticas de seguridad.
b. La Sub Gerencia de Logística para conocimiento y fines.
c. La Oficina de Seguridad y Defensa Nacional para su conocimiento y fines.

7.2 DE LA CONEXIÓN A LA RED DEL RENIEC DE DISPOSITIVOS MÓVILES DEL PERSONAL ADMINISTRADOR DE SERVICIOS CRÍTICOS

7.2.1 El acceso a la red de los dispositivos móviles del personal administrador de servicios críticos, es autorizado por el correspondiente Sub Gerente.

Las credenciales respectivas deben ser solicitadas a través del "Software de Gestión de Incidentes" de la Sub Gerencia de Soporte Técnico Operativo por el personal administrador de servicios críticos.

Los dispositivos móviles de los funcionarios con niveles de Gerente, Sub Gerente o Jefes Regionales y personal administrador de servicios críticos que tienen acceso a la red del RENIEC deben tener instalado el

antivirus institucional y cumplir con todas las directivas y políticas de seguridad informática.

7.3 DE LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES Y SU CONTENIDO FUERA DE LAS INSTALACIONES DEL RENIEC

7.3.1 El uso de dispositivos móviles fuera del ámbito de la Institución debe ser autorizado por el área responsable. La seguridad provista debe ser equivalente a la suministrada dentro de la Institución teniendo en cuenta los riesgos de trabajar fuera de la red del RENIEC. Los usuarios deben tomar en cuenta los riesgos de seguridad tales como robo o interceptación de información, los cuales pueden variar considerablemente según las ubicaciones.

7.3.2 Se debe considerar los siguientes lineamientos:

a. Los dispositivos móviles utilizados en lugares públicos deben estar al alcance del usuario asignado. Para su transporte se debe contar con el equipaje de mano adecuado.
b. Se deben respetar las recomendaciones del fabricante como la protección por exposición a campos electromagnéticos fuertes.

7.4 DE LA CONEXIÓN DE DISPOSITIVOS MÓVILES DE PROVEEDORES O VISITANTES A LA RED DEL RENIEC Y/O SU SERVICIO DE INTERNET

DE LOS PROVEEDORES CON CONTRATO VIGENTE

7.4.1 La conexión de los dispositivos móviles de proveedores con contrato vigente a la red inalámbrica o alámbrica del RENIEC y/o su servicio de Internet, debe solicitarse por el área responsable mediante el "Software de Gestión de Incidentes" de la Sub Gerencia de Soporte Técnico Operativo, sustentando el motivo de la solicitud y trabajos.

7.4.2 El área solicitante es responsable de la actividad del proveedor y del buen uso del servicio habilitado durante la permanencia en las instalaciones del RENIEC. Todo dispositivo móvil debe cumplir con las políticas definidas en las directivas DI-328-GTI/022 "Seguridad Informática de la Red del RENIEC" y/o DI-327-GTI/021 "Servicios de Comunicación para Usuarios Finales", numeral 6.4 Del servicio de Acceso a Internet.

DE LOS VISITANTES

7.4.3 El acceso al servicio de Internet de los dispositivos móviles de un visitante (persona natural o jurídica, sin contrato vigente con el RENIEC), debe solicitarse por el área responsable mediante el "Software de Gestión de Incidentes" de la Sub Gerencia de Soporte Técnico Operativo, sustentando el motivo de la solicitud, con un día de anticipación.

7.4.4 El área solicitante es responsable del buen uso del servicio habilitado durante la permanencia en las instalaciones del RENIEC. Todo dispositivo móvil debe cumplir con las políticas y directivas de Seguridad indicadas en el numeral "6.4 Servicio de Acceso a Internet" de la Directiva DI-327-GTI/021 "Servicios de Comunicación para Usuarios Finales".

VIII. DISPOSICIONES COMPLEMENTARIAS

8.1 La Gerencia de Tecnología de la Información, a través de la Sub Gerencia de Operaciones Telemáticas, y en coordinación con la Escuela Registral, promueve y organiza 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. ANEXO

ANEXO N° 01

FORMATO DE EVALUACIÓN DE DISPOSITIVOS MÓVILES EXTERNOS

RENIEC

REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

FORMATO DE EVALUACIÓN DE DISPOSITIVOS MÓVILES EXTERNOS

DATOS DEL FORMATO
CÓDIGO: GC-T-F-EDM-07/SGOT/GTI/RE Versión: 01 Fecha Emisión: 11/12/2017 Fecha Actualización: 11/12/2017

N° Formato: 00001/SGOT/GTI FECHA DE EVALUACIÓN: 11/12/2017

DATOS DEL EVALUADOR

GERENCIA:	Gerencia de Tecnología de la Información
SUB GERENCIA	Sub Gerencia de Operaciones Telemáticas
NOMBRES Y APELLIDOS:	Carlos Mesa Loyola
CARGO/ROL:	Especialista de Seguridad Informática

DATOS DEL FORMATO DE SOLICITUD:

NUMERO DE FORMATO	0056	FECHA DE SOLICITUD	11/12/2017
NOMBRE DEL GERENTE	GILBERTO PALOMINO		
GERENCIA	ADMINISTRACIÓN		

DATOS DEL USUARIO EXTERNO:

NOMBRES Y APELLIDOS:	Sandra Rivas			
CARGO	Auditor de Sistemas			
INSTITUCIÓN	Pública	X	Privada	☐
NOMBRE DE LA INSTITUCIÓN	Contraloria Pública			

VERIFICACIÓN DEL DISPOSITIVO MÓVIL:

Controles de Seguridad:	SI	No
a) Cuenta con Antivirus	☐	☐
b) Cuenta con Sistema Operativo Actualizado	☐	☐
c) Cuenta con Programas Originales	☐	☐
d) Cuenta con otros aplicativos de seguridad	☐	☐

Nota: Se conectará a la red si solo sí, las condiciones a) y b) son afirmativas.

Comentarios:

GERENCIA DE PLANIFICACIÓN Y PRESUPUESTO

GERENCIA DE TECNOLOGÍA DE LA INFORMACIÓN

SUB GERENTE DE OPERACIONES TELEMÁTICAS

SUB GERENCIA DE ASESORÍA ADMINISTRATIVA

GERENCIA ASESORÍA JURÍDICA

SECRETARÍA GENERAL

ANEXO Nº 02

CUADRO DE CONTROL DE CAMBIOS

"USO DE DISPOSITIVOS MÓVILES EN EL 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
No existía en esta versión	Numeral 3.5
No existía en esta versión	Numeral 3.6
Numeral 3.6	Numeral 3.7
Numeral 3.7	Eliminado
Numeral 3.8	Eliminado
Numeral 3.9	Numeral 3.8
No existía en esta versión	Numeral 3.9
Numeral 3.10	Eliminado
Numeral 3.11	Eliminado
Numeral 3.12	Numeral 3.10
Numeral 3.13	Numeral 3.11
No existía en esta versión	Numeral 3.12
Numeral 3.14	Numeral 3.13
IV. DEFINICIÓN DE TERMINOS	**IV. DEFINICIÓN DE TERMINOS**
Numeral 4.6	Numeral 4.1
Numeral 4.7	Numeral 4.2
Numeral 4.1	Numeral 4.3
Numeral 4.2	Numeral 4.4
Numeral 4.3	Numeral 4.5
Numeral 4.4	Numeral 4.6
Numeral 4.8	Numeral 4.7
No existía en esta versión.	Numeral 4.8
Numeral 4.5	Numeral 4.9
Numeral 4.9	Numeral 4.10
No existía en esta versión.	Numeral 4.11
V. RESPONSABILIDADES	**V. RESPONSABILIDADES**
Numeral 5.2	Numeral 5.2
Numeral 5.4	Numeral 5.4
No existía en esta versión	Numeral 5.5
Numeral 5.6	Numeral 5.6
VI. DISPOSICIONES GENERALES	**VI. DISPOSICIONES GENERALES**
Numeral 6.1	Numeral 6.1
Numeral 6.2	Eliminado
6.3 DEL ACCESO A LA RED DEL RENIEC, DE LAS	**6.2 DEL ACCESO A LA RED DEL RENIEC, DE LAS CONTRASEÑAS Y SEGURIDAD EN LOS DISPOSITIVOS**

"USO DE DISPOSITIVOS MÓVILES EN EL RENIEC"	
IDENTIFICACIÓN DEL CAMBIO	
NUMERAL VIGENTE	**NUMERAL MODIFICADO**
CONTRASEÑAS Y SEGURIDAD EN LOS DISPOSITIVOS MÓVILES DE PROPIEDAD DEL RENIEC	**MÓVILES DE PROPIEDAD DEL RENIEC**
Numeral 6.3.1	Numeral 6.2.1
Numeral 6.3.2	Numeral 6.2.2
Numeral 6.3.3	Numeral 6.2.3
Numeral 6.3.4	Numeral 6.2.4
6.4 DE LA CONEXIÓN A LA RED DEL RENIEC DE DISPOSITIVOS MÓVILES DEL PERSONAL ADMINISTRADOR DE SERVICIOS CRÍTICOS	**6.3 DE LA CONEXIÓN A LA RED DEL RENIEC DE DISPOSITIVOS MÓVILES DEL PERSONAL ADMINISTRADOR DE SERVICIOS CRÍTICOS**
Numeral 6.4.1	Numeral 6.3.1
Numeral 6.4.2	Eliminado
6.5 DE LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES Y SU CONTENIDO FUERA DE LAS INSTALACIONES DEL RENIEC	**6.4 DE LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES Y SU CONTENIDO FUERA DE LAS INSTALACIONES DEL RENIEC**
Numeral 6.5.1	Numeral 6.4.1
Numeral 6.5.2	Numeral 6.4.2
6.6. DE LA CONEXIÓN DE DISPOSITIVOS MÓVILES DE PROVEEDORES O VISITANTES A LA RED DEL RENIEC Y/O SU SERVICIO DE INTERNET	**6.5. DE LA CONEXIÓN DE DISPOSITIVOS MÓVILES DE PROVEEDORES O VISITANTES A LA RED DEL RENIEC Y/O SU SERVICIO DE INTERNET**
Numeral 6.6.1	Numeral 6.5.1
Numeral 6.6.2	Numeral 6.5.2
Numeral 6.6.3	Eliminado
No existía en esta versión	Numeral 6.5.3
VII. DISPOSICIONES ESPECIFICAS	**VII. DISPOSICIONES ESPECIFICAS**
7.1.1 DEL ACCESO A LA RED DEL RENIEC	**7.1.1 DEL ACCESO A LA RED DEL RENIEC**
Numeral 7.1.1.1	Numeral 7.1.1.1
Numeral 7.1.1.2	Numeral 7.1.1.2
Numeral 7.1.1.3	Numeral 7.1.1.3
7.1.2 DE LAS CONTRASEÑAS Y SEGURIDAD EN LOS DISPOSITIVOS MÓVILES	**7.1.2 DE LAS CONTRASEÑAS Y SEGURIDAD EN LOS DISPOSITIVOS MÓVILES**
Numeral 7.1.2.1	Numeral 7.1.2.1
Numeral 7.1.2.2	Numeral 7.1.2.2
Numeral 7.1.2.3	Numeral 7.1.2.3
7.2 DE LA CONEXIÓN A LA RED DEL RENIEC DE DISPOSITIVOS	**7.2 DE LA CONEXIÓN A LA RED DEL RENIEC DE DISPOSITIVOS MÓVILES DEL PERSONAL ADMINISTRADOR**

"USO DE DISPOSITIVOS MÓVILES EN EL RENIEC"	
IDENTIFICACIÓN DEL CAMBIO	
NUMERAL VIGENTE	**NUMERAL MODIFICADO**
MÓVILES DEL PERSONAL ADMINISTRADOR DE SERVICIOS CRÍTICOS	**DE SERVICIOS CRÍTICOS**
Numeral 7.2.1	Numeral 7. 2.1
7.3 DE LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES Y SU CONTENIDO FUERA DE LAS INSTALACIONES DEL RENIEC	**7.3 DE LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES Y SU CONTENIDO FUERA DE LAS INSTALACIONES DEL RENIEC**
Numeral 7.3.1	Numeral 7.3.1
Numeral 7.3.2	Numeral 7.3.2
7.4 DE LA CONEXIÓN DE DISPOSITIVOS MÓVILES DE PROVEEDORES O VISITANTES A LA RED DEL RENIEC Y/O SU SERVICIO DE INTERNET	**7.4DE LA CONEXIÓN DE DISPOSITIVOS MÓVILES DE PROVEEDORES O VISITANTES A LA RED DEL RENIEC Y/O SU SERVICIO DE INTERNET**
DE LOS PROVEEDORES	**DE LOS PROVEEDORES CON CONTRATO VIGENTE**
Numeral 7.4.1	Numeral 7.4.1
Numeral 7.4.2	Numeral 7.4.2
DE LOS VISITANTE	**DE LOS VISITANTES**
Numeral 7.4.3	Numeral 7.4.3
Numeral 7.4.4	Numeral 7.4.4
No existía en esta versión.	**VIII.DISPOSICIONES COMPLEMENTARIAS**
No existía en esta versión.	Numeral 8.1
VIII. VIGENCIA	**IX. VIGENCIA**
IX. APROBACIÓN	**X. APROBACIÓN**
X. ANEXOS	**XI. ANEXOS**
No existía en esta versión.	Anexo N° 01
Anexo N° 01	Anexo N° 02