DIRECTIVA

SERVICIOS DE COMUNICACIÓN PARA USUARIOS FINALES

RESOLUCIÓN SECRETARIAL N° 97 -2018/SGEN/RENIEC		
DI-327-GTI/021	VERSIÓN: 04 N° PÁGINAS: 48	FECHA DE APROBACIÓN 10 JUL. 2018

INDICE

GERENCIA ASESORÍA JURÍDICA

I. OBJETIVO

Establecer los lineamientos para el uso de los servicios de Perfil de Dominio, Correo Electrónico, Mensajería Interna (Messenger), acceso a Internet, Telefonía IP, Infraestructura de Comunicación, Videoconferencia, VPN, evaluación y análisis de vulnerabilidades de los servicios y/o aplicaciones web y publicación a internet de los servicios y/o aplicaciones web, con el fin de garantizar su uso correcto, manteniendo de manera eficiente la operatividad de la red, así como contribuir con la gestión de la seguridad de la información, la integridad de las redes y los servicios a nivel nacional por parte de los usuarios autorizados del Registro Nacional de Identificación y Estado Civil - RENIEC.

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 por todos los usuarios de los servicios de Perfil de Dominio, Correo Electrónico, Mensajería Interna (Messenger), acceso a Internet, Telefonía IP, Infraestructura de Comunicación, Videoconferencia y VPN de las diferentes áreas del RENIEC.

Asimismo, a los usuarios de la Sub Gerencia de Ingeniería de Software que solicitan la evaluación y análisis de vulnerabilidades de los servicios y/o aplicaciones web y solicitudes de publicación a internet.

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° 28530,** Ley de promoción de acceso a Internet para personas con discapacidad y de adecuación del espacio físico en cabinas públicas de Internet, del 25 de mayo de 2005 y sus modificatorias.

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

3.5 **Ley N° 28716,** Ley de Control Interno de las Entidades del Estado, del 18 de abril de 2006, y sus modificatorias.

3.6 **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.

3.7 **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 y sus modificatorias.

3.8 **Decreto Supremo N° 031-2005-MTC,** aprueba el Reglamento de la Ley N° 28493 que regula el envío del correo electrónico comercial no solicitado (SPAM), del 04 de enero de 2006.

3.9 **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.

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

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

3.12 **Resolución N° 001-2007/INDECOPI-CTR,** aprueba Normas Técnicas Peruanas, del 22 de enero de 2007.

3.13 **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.

3.14 **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.

3.15 **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.

3.16 **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.

3.17 **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.

3.18 **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 del 2016 y su modificatorias.

3.19 **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.

3.20 **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 Alta del Servicio de Mensajería (Messenger)

Proceso mediante el cual se habilita el servicio de acuerdo al perfil de usuario solicitado.

4.2 Áreas

Nombre genérico y que indistintamente hace mención tanto a órganos como unidades orgánicas de una entidad de la Administración Pública (Art. 5° del D.S. N° 043-2006-PCM).

4.3 Baja de Servicio de Correo Electrónico

Proceso mediante el cual se elimina un buzón registrado, suprimiendo el servicio.

4.4 Baja de Servicio de Mensajería (Messenger)

Proceso mediante el cual se elimina el servicio en la cuenta registrada.

4.5 Buzón de correo electrónico

Cuenta registrada en el servidor de correo, destinada a almacenar los mensajes que recibe un usuario, hasta que estos sean leídos o descargados por el cliente de correo.

4.6 Buzón de correo electrónico Adicional

Es aquel asociado a un determinado servicio y que tiene un nombre relacionado a una determinada función/rol dentro de la Institución (Ejemplos: HELPDESK – Mesa de Ayuda, CEL – Consultas en Línea, CONSULTAS – Consultas Ciudadanos, etc.).

4.7 Carpeta Personal

Archivo con extensión "pst" localizado en el disco duro de la computadora del usuario. Contiene todos los mensajes y archivos adjuntos que fueron descargados directamente del buzón del usuario de una cuenta de correo electrónico.

4.8 Cliente VPN

Software propietario de la plataforma que soporta el servicio VPN y que hace posible el establecimiento de un canal de comunicación seguro, a través de internet, entre la computadora remota y el servidor VPN.

4.9 Cuenta de usuario

Las cuentas de usuario de Directorio Activo (Active Directory) representan entidades físicas (como personas) o también denominadas entidades de seguridad. Las entidades de seguridad son objetos de directorio a los que se asignan automáticamente identificadores de seguridad (SID), que se usan para acceder a recursos del dominio

4.10 Dominio

Nombre alfanumérico único que identifica un sitio web en internet. El nombre de dominio se adquiere en forma exclusiva, para ser usada en todo el mundo.

4.11 Grupo de Distribución

Es una agrupación de usuarios de correo electrónico que permite que cada integrante reciba una copia del mensaje enviado al Grupo de Distribución.

4.12 Grupo de Distribución Interno

Es una agrupación de usuarios de correo electrónico dentro de un área de trabajo que permite la comunicación interna entre ellos.

4.13 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.

4.14 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.

4.15 Messenger

Programa que permite la comunicación en tiempo real por medio de mensajes escritos con personas previamente autorizadas. Permite además la transferencia de archivos y la realización de video conferencias.

4.16 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.

4.17 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. La responsabilidad en ningún caso es delegable.

4.18 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.

4.19 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.

4.20 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.

4.21 Suspensión de un Perfil / Cuenta de correo electrónico

Proceso mediante el cual, a solicitud del responsable del área que autoriza, se deshabilita y/o suspende temporalmente un perfil o buzón, por motivos de vacaciones, descanso médico y/o viaje del usuario.

4.22 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.

4.23 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.

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 Sub Gerencia de Operaciones Telemáticas (SGOT) de la GTI, administrar adecuadamente los servicios de Perfil de Dominio, Correo Electrónico, Mensajería Interna (Messenger), Acceso a Internet, Telefonía IP, Infraestructura de Comunicación, Videoconferencia y VPN a los usuarios autorizados del Registro Nacional de Identificación y Estado Civil – RENIEC; estableciendo controles, en función a los recursos y capacidades disponibles, para garantizar la seguridad informática en estos servicios.

5.3. Es responsabilidad de cada unidad orgánica elevar sus solicitudes y/o requerimientos de los servicios de Perfil de Dominio, Correo Electrónico, Mensajería Interna (Messenger), Acceso a Internet, Telefonía IP, Infraestructura de Comunicación, Videoconferencia y VPN a través del "Software de Gestión de Incidentes", a la Sub Gerencia de Operaciones Telemáticas.

5.4. Es responsabilidad de la Sub Gerencia de Operaciones Telemáticas atender las solicitudes de requerimientos de los servicios de las distintas áreas a través del "Software de Gestión de Incidentes", en un tiempo no mayor a las 48 horas para los servicios de Perfil de Dominio, Correo Electrónico, Mensajería Interna (Messenger), Acceso a Internet, Telefonía IP, Infraestructura de Comunicación, Videoconferencia y VPN.

5.5. Es responsabilidad de los Gerentes, Jefes de Oficinas, Sub Gerentes y Jefes Regionales, brindar la autorización adecuada de los servidores civiles a su cargo, a los siguientes servicios de comunicación para usuarios finales: Perfil de Dominio, Correo Electrónico, Mensajería Interna (Messenger), Acceso a Internet, Telefonía IP, Infraestructura de Comunicación, Videoconferencia y VPN; con el fin de contribuir en el desarrollo y cumplimiento de sus actividades.

5.6. Es responsabilidad de los Gerentes, Jefes de Oficinas, Sub Gerentes y Jefes Regionales, definir una adecuada distribución de los puntos de red para los servidores civiles a su cargo, con la finalidad de evitar continuos requerimientos de desplazamientos de red en el área, lo cual incurre en gastos de material y mano de obra.

5.7. Es responsabilidad de los Gerentes que soliciten el servicio VPN para los administradores de servicios críticos y registradores; velar por el uso adecuado de este servicio por parte de su personal.

5.8. Es responsabilidad de los usuarios finales que cuentan con los servicios de Perfil de Dominio, Correo Electrónico, Mensajería Interna (Messenger), Acceso a Internet, Telefonía IP, Infraestructura de Comunicación, Videoconferencia y VPN cumplir con las disposiciones establecidas en la

presente Directiva. Se suspende el servicio cuando se detecta un mal uso e incumplimiento de las disposiciones señaladas en la presente Directiva.

En caso de incumplimiento, la Sub Gerencia de Operaciones Telemáticas comunica, mediante informe técnico, a la GTI con copia a la Gerencia de Talento Humano (GTH) para la evaluación y acciones pertinentes.

5.9. Es responsabilidad de la GTH, a través de la Sub Gerencia de Personal (SGPS), comunicar a la GTI sobre la baja y movimientos de los servidores civiles dentro de la institución en un plazo de dos (02) días hábiles para facilitar la correcta administración de todos los "Servicios de Comunicación para Usuarios Finales".

5.10. Es responsabilidad de cada unidad orgánica solicitar a la GTI la suspensión temporal de los servicios de comunicación, en un plazo no mayor a 48 horas de iniciado su periodo vacacional, licencias por enfermedad y todas aquellas situaciones que impliquen ausencia o no asistencia de los servidores civiles.

5.11. Es responsabilidad de las unidades orgánicas revisar al cierre del año y ratificar, en caso corresponda, los servicios de comunicaciones otorgados a sus servidores civiles incluyendo permisos y privilegios por cada usuario. La ratificación se informa mediante memorando dirigido a la GTI, adjuntando el "Formato para Ratificación de Servicios de Comunicación para Usuarios Finales" (Anexo N° 10) firmado digitalmente por el Gerente y/o Jefe de Oficina.

5.12. Es responsabilidad de la Sub Gerencia de Ingeniería de Software (SGIS) solicitar el análisis de vulnerabilidades de los servicios y/o aplicaciones web, así como su publicación o baja en internet cuando se requiera; previa coordinación con la Sub Gerencia de Operaciones Telemáticas.

VI. DISPOSICIONES GENERALES

6.1. DEL SERVICIO DE PERFIL DE DOMINIO

6.1.1 La Sub Gerencia de Operaciones Telemáticas es la encargada de la gestión del Perfil de Dominio para los servidores civiles del RENIEC.

6.1.2 La incorporación de cada servidor civil sobre el dominio de red del RENIEC, involucra la asignación de un Perfil de Dominio, el mismo que representa la identificación digital, a través de la cual el servidor civil puede hacer uso de los diferentes recursos informáticos de la red.

6.1.3 La política para creación del Perfil de Dominio se encuentra en la Directiva DI-328-GTI/022 "Seguridad Informática de la Red del RENIEC", numeral 7.3.1 "Del control de accesos a los servicios de Red".

6.1.4 La identificación digital de cada servidor civil es única e intransferible. Es responsabilidad del servidor civil conservar su identificación digital en secreto por ser de uso personal y exclusivo; asimismo, debe cumplir con las políticas de control de acceso, seguridad y uso de la red detalladas en la presente Directiva.

6.1.5 Todo servidor civil del RENIEC, puede hacer uso de un Perfil de Dominio (cuenta de usuario), previa autorización y requerimiento del área responsable.

6.1.6 Se encuentra prohibido el intento de transgresión a la seguridad de las cuentas de usuario de dominio. En caso ocurra algún incidente de

seguridad, vulnerando a una cuenta de usuario que no le pertenezca, el servidor civil que origine el incidente de seguridad es el responsable directo del hecho y de la cuenta vulnerada, la cual se deshabilita mientras dure la auditoría correspondiente.

Toda transgresión a la seguridad de las cuentas de usuario de dominio es sometida a una auditoría a cargo de la Sub Gerencia de Operaciones Telemáticas, que concluye con la emisión de un informe técnico a la GTI con copia a la GTH para su evaluación y acciones pertinentes.

6.1.7 Los servidores civiles poseedores de cuentas de usuario deben tomar las medidas que se mencionan en la Directiva DI-328-GTI/022 "Seguridad Informática de la Red del RENIEC", numeral 7.3.1.7 las cuales están especificadas para garantizar su inviolabilidad y uso personal.

6.1.8 Al usuario que utilice de forma inadecuada los recursos de red (o se detecte que está instalando o utilizando herramientas de hacking o intrusión), se retira de la red mientras se realiza la auditoría técnica por los especialistas de seguridad informática de la Sub Gerencia de Operaciones Telemáticas, la cual concluye con la emisión de un informe técnico a la GTI con copia a la GTH informando del hecho para su evaluación y acciones pertinentes.

6.2 DEL SERVICIO DE CORREO ELECTRÓNICO

6.2.1 El servicio de correo electrónico, es un recurso que brinda el RENIEC únicamente a los servidores civiles para uso exclusivo en las actividades laborales y/o responsabilidades asignadas al cargo y/o roles que ocupa dentro de la institución.

6.2.2 El nombre de la cuenta de correo electrónico institucional para cada usuario está formado por el nombre del perfil de dominio, ligado con el símbolo @ al nombre de dominio de la institución (establecido por la Directiva N° 010-2002-INEI/DTNP "Normas Técnicas para la Asignación de Nombres de Dominio de las Entidades de la Administración Pública").

6.2.3 La cuenta de correo electrónico es personal e intransferible, asimismo el tener una cuenta de correo electrónico institucional compromete y obliga a cada usuario a aceptar y cumplir las normas establecidas por la institución.

6.2.4 Queda prohibido el uso del servicio de correo electrónico para las actividades o acciones que se detallan a continuación:

a. Enviar mensajes con propósito político, comercial o financiero ajeno a la institución.

b. Participar en la propagación de mensajes "cadena" o en esquemas piramidales o similares.

c. Distribuir mensajes con contenidos inapropiados y/o lesivos a la moral. Por ejemplo: apología del terrorismo, uso y/o distribución de programas piratas, pornografía, pedofilia amenazas, estafas, esquemas de enriquecimiento piramidal, virus o código hostil en general.

d. Falsificar las cuentas de correo electrónico o editar el contenido de un mensaje de manera malintencionada con el propósito de reenviarlo.

e. Enviar de forma masiva publicidad o cualquier otro tipo de correo electrónico no solicitado o correo basura (SPAM).

f. Suscribirse a listas de interés de temas no relacionados con su labor profesional o cualquier otra fuente de información no relacionada con las actividades propias de la Institución.

g. Facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas.

h. El envío de mensajes a foros de discusión (listas de distribución y/o newsgroups) que comprometan la información de la institución o violen las leyes del Estado Peruano.

i. El envío de mensajes de correo electrónico entre los servidores civiles de la institución y otras personas que no pertenezcan al RENIEC, en los cuales se divulguen, comenten o expresen hechos, opiniones o cualquier tipo de información relacionada a controversias, problemas, funcionamiento, políticas, personas o cualquier otra situación o asunto interno del RENIEC, que puedan poner en entredicho la reputación o imagen institucional; aunque la información divulgada no sea de naturaleza confidencial.

j. Dirigir a un usuario o a varios usuarios mensajes que tengan el objetivo de sobrecargar el servicio poniendo en riesgo la continuidad del mismo.

Cualquier incidente provocado por la ejecución de alguna de estas acciones es de entera responsabilidad del usuario responsable de la cuenta de correo electrónico asignada.

6.2.5 Cuando un usuario realice algunas de las actividades o acciones mencionadas en el numeral 6.2.4, es sometido a una investigación y auditoría técnica a cargo de los especialistas de seguridad informática de la Sub Gerencia de Operaciones Telemáticas; la investigación concluye con la emisión de un informe técnico a la GTI con copia a la GTH informando del hecho para su evaluación y acciones pertinentes.

6.2.6 Un Grupo de Distribución y/o correo electrónico adicional es creado solo cuando su alcance sea de interés institucional. Antes de solicitar la creación de un Grupo de Distribución, se debe coordinar con el responsable de la administración del servicio de correo electrónico para la definición del nombre.

6.2.7 El buzón del correo electrónico adicional se configura localmente en el cliente Outlook de la computadora asignada a los servidores civiles que así lo requieran para el cumplimiento de sus funciones. Las respuestas a los mensajes recibidos en el buzón del correo electrónico adicional son emitidas a nombre de los servidores civiles.

6.2.8 A fin de garantizar el normal funcionamiento de los sistemas de correo electrónico, la Sub Gerencia de Operaciones Telemáticas define los tamaños máximos de archivos a enviar/recibir, así como los límites de almacenamiento.

Cuando un buzón esté por alcanzar el límite de almacenamiento, los administradores del servicio notifican al usuario mediante mensaje de correo electrónico para que tome las acciones correctivas y evite la suspensión del servicio de correo electrónico.

Cuando un buzón sobrepase el límite de almacenamiento, el servicio de correo es suspendido automáticamente. En este caso los administradores del servicio notifican esta situación al usuario mediante mensaje de correo electrónico, quien debe liberar el espacio utilizado por su buzón para luego solicitar la reanudación del servicio. El usuario final debe solicitar a Mesa de Ayuda la configuración del autoarchivado de sus mensajes y las reglas correspondientes para evitar futuras suspensiones del servicio.

6.2.9 El permiso para envío de mensajes al Grupo RENIEC está restringido y solo puede ser solicitado mediante- documento dirigido a la GTI, el cual es proveído a la Sub Gerencia de Operaciones Telemáticas para su evaluación y atención, de ser el caso. Los archivos adjuntos al correo electrónico no deben superar los 500 KB, caso contrario se deben, utilizar hipervínculos que permitan a los interesados descargar el contenido.

6.2.10 Cuando el usuario deje de usar su computadora, debe bloquear la sesión de trabajo abierta, a fin de evitar que un tercero tenga acceso no autorizado o use su cuenta de correo electrónico. Adicionalmente, se ha implementado un protector de pantalla institucional, el cual se activa transcurridos diez minutos de inactividad en la computadora bloqueando el acceso.

6.2.11 La Sub Gerencia de Soporte Técnico Operativo (SGSTO) configura la entrega (copia) de mensajes en la computadora del usuario, ya sea hacia una carpeta personal (archivo de extensión pst y ost), o mediante la configuración del autoarchivado de mensajes y/o creación de reglas en la bandeja de entrada. A partir de ese momento el usuario es responsable por el contenido de sus mensajes así como de su integridad y disponibilidad.

6.2.12 Los usuarios del servicio de correo electrónico, bajo responsabilidad, deben abrir su buzón al menos una vez a la semana, depurando su contenido y trasladando a carpetas personales aquellos mensajes que requiera conservar. Si un usuario no accede regularmente a su casilla de correo electrónico, el espacio de almacenamiento en el servidor es ocupado por completo por los mensajes recibidos y no leídos, circunstancia bajo la cual el usuario ya no puede recibir mensajes.

6.2.13 Por defecto, el ingreso y salida de mensajes provenientes de servidores gratuitos (Hotmail, Gmail, Yahoo y otros) al correo electrónico institucional está bloqueado para todos los servidores civiles del RENIEC. Los funcionarios de la Alta Dirección, Jefes de Oficinas, Gerentes, Sub Gerentes y Jefes Regionales pueden solicitar la autorización para recibir y remitir mensajes de servidores gratuitos en sus buzones de correo electrónico, sustentando la necesidad y haciendo mención específica del "permiso para recepción y envío de mensajes de correo electrónico provenientes y destinados desde y hacia servidores gratuitos", mediante el envío de un memorando a la

GTI, quien provee a la Sub Gerencia de Operaciones Telemáticas para su evaluación y atención en caso corresponda.

6.2.14 La Sub Gerencia de Operaciones Telemáticas monitorea permanente el estado de los buzones de correo electrónico y está facultada a suspender los buzones de correo electrónico bajo las siguientes condiciones:

a. Cuando el buzón ocupe todo el espacio de almacenamiento reservado en el servidor (buzón lleno). Los mensajes no se pueden recuperarse.

b. Por incumplimiento del numeral 6.4.2

6.2.15 La Sub Gerencia de Operaciones Telemáticas realiza la configuración del correo institucional en los teléfonos inteligentes (smartphones) proporcionados por el RENIEC, en los siguientes casos:

a. Funcionarios de la Alta Dirección, Jefes de Oficinas, Gerentes, Sub Gerentes y Jefes Regionales que lo soliciten a través de correo electrónico.

b. Administradores de Servicios Críticos de las Sub Gerencias de Operaciones Telemáticas, Soporte Técnico Operativo, Gestión de Bases de Datos de la GTI y Jefes de Proyecto de la Sub Gerencia de Ingeniería Software, solicitados a través del Jefe inmediato mediante correo electrónico.

c. A los usuarios que son responsables de actividades críticas en las diferentes unidades orgánicas, que son solicitados a través del Jefe inmediato mediante Memorando dirigido a la GTI con la justificación respectiva, para la correspondiente evaluación por parte de la Sub Gerencia de Operaciones Telemáticas.

6.2.16 El acceso al servicio de correo electrónico mediante teléfonos inteligentes (smartphones) constituye una facilidad que permite al usuario leer y enviar correos electrónicos cuando se encuentre fuera del centro de labores.

6.3 DEL SERVICIO DE MESSENGER INTERNO

6.3.1 El servicio de mensajería instantánea (Messenger Interno) asignado a los servidores civiles autorizados, es para uso exclusivo de las actividades laborales y/o vinculadas a las actividades propias de la institución. En consecuencia, el servicio no debe ser utilizado para:

6.3.1.1 Enviar información para cualquier propósito político, comercial o financiero ajeno a la Institución.

6.3.1.2 Enviar mensajes con contenidos inapropiados. Por ejemplo: apología del terrorismo, uso y/o distribución de programas piratas, pornografía, pedofilia amenazas, estafas, esquemas de enriquecimiento piramidal, virus o código hostil en general.

6.3.2 El servicio de mensajería instantánea (Messenger Interno) permite a un usuario la comunicación con personal interno de la institución,

logrando transmitir y compartir información con otros usuarios autorizados.

6.4 DEL SERVICIO DE ACCESO A INTERNET

6.4.1 La Sub Gerencia de Operaciones Telemáticas es la unidad orgánica encargada de la administración del acceso a internet, reservándose el derecho de monitorear el uso de este servicio, tomando las acciones que sean necesarias para asegurar la confiabilidad del servicio, en función a los recursos y capacidades disponibles.

6.4.2 El uso de internet está prohibido para fines personales ajenos a los objetivos institucionales del RENIEC. El acceso a internet es un recurso que brinda la institución a todos los servidores civiles autorizados, para el desarrollo de actividades estrictamente relacionadas al entorno laboral con las responsabilidades asignadas al cargo que ocupa.

6.4.3 Las unidades orgánicas deben priorizar la asignación del acceso al servicio de internet al servidor civil que cumple labores de asesoría e investigación y a todo aquel que mediante el acceso al servicio de Internet le permita contribuir con el desarrollo y cumplimiento de las actividades que le son asignadas.

6.4.4 Se encuentra prohibido el uso de software y/o hardware no autorizados por la GTI o la modificación de las configuraciones establecidas en los equipos informáticos, para evitar los controles de seguridad del servicio de internet. Así mismo, se prohíbe el uso de herramientas de hacking dentro de la red, a los usuarios no autorizados por la GTI, que atente contra la seguridad de la información del RENIEC y la seguridad de las diferentes instituciones y empresas que publican sus servicios web en internet.

6.4.5 Se encuentra prohibido el acceso a páginas web de contenido pornográfico, actividades ilegales (drogas, terrorismo, cibercrímenes, ciberdelitos, hacktivismo, etc.), aplicaciones P2P, sites de contenido malicioso y aplicaciones para realizar ataques informáticos a sites y hosts de internet. Están restringidas las páginas web de ocio y entretenimiento (juegos en línea, redes sociales, comunidades de chat, música online, videos, tv online, etc.), aplicaciones de acceso remoto a través de internet, almacenamiento en la nube, acceso a servidores de correo electrónico gratuito u otros servicios y aplicaciones que no concuerden con las actividades para las que el RENIEC ha dispuesto el servicio de acceso a internet.

6.4.6 Si para el desarrollo de sus funciones el usuario requiere acceder a páginas de contenido multimedia (música y video), redes sociales, servicios y/o aplicaciones de almacenamiento en la nube, acceso a servidores de correo electrónico gratuito u otras aplicaciones restringidas; el órgano responsable debe solicitar mediante un memorando dirigido a la GTI, justificando la necesidad de acceso e indicando las páginas, aplicaciones y/o servicios específicos que se deben habilitar para el usuario.

6.4.7 El acceso remoto de aplicaciones a través de internet está permitido sólo a los usuarios de la GTI que administran soluciones tecnológicas críticas, por motivos y facilidades de soporte técnico; el acceso a esta

aplicación se solicita mediante correo electrónico del Jefe inmediato a la Sub Gerencia de Operaciones Telemáticas. Para el uso de esta aplicación por usuarios de otra unidad orgánica, se solicita el acceso mediante memorando dirigido a la GTI sustentando el motivo y remitiendo la relación de usuarios autorizados, los cuales no deben exceder en número de cinco por unidad orgánica.

La Sub Gerencia de Operaciones Telemáticas evalúa los riesgos y en caso sea necesario incorpora mecanismos disponibles que permitan asegurar la confidencialidad e integridad de la información.

6.4.8 Para la descarga de archivos y/o programas desde internet, se debe tener presente las consideraciones expuestas en la Directiva DI-328-GTI/022 "Seguridad Informática de la Red del RENIEC", numeral 7.6.2.5.

6.4.9 La información consultada mediante el uso de internet, debe apoyar directamente las funciones relacionadas con el campo de la responsabilidad laboral del usuario o servir como herramienta para su desempeño o para el cumplimiento de las actividades de su área, según sea el caso.

6.5 DEL SERVICIO DE TELEFONÍA IP

6.5.1 La Sub Gerencia de Operaciones Telemáticas es la unidad orgánica responsable de la administración del servicio de telefonía IP, tomando las acciones que sean necesarias para asegurar la confiabilidad del servicio en función a los recursos y capacidades disponibles.

6.5.2 El servicio de telefonía IP es un recurso que brinda el RENIEC a los servidores civiles para el desarrollo de las actividades y responsabilidades asignadas en su entorno laboral.

6.5.3 Todo usuario o grupo de usuarios antes de realizar cambios, traslados o modificaciones dentro de su ambiente de trabajo que involucren reubicación o habilitación de nuevas líneas o equipos de telefonía, debe coordinar inicialmente con la Sub Gerencia de Operaciones Telemáticas, a fin de evaluar la factibilidad de los cambios solicitados, para prevenir el deterioro, corte o la mala utilización del punto de red y/o equipo existente.

6.5.4 En caso de falla/avería en el funcionamiento del equipo, se debe reportar a Mesa de Ayuda o a través del *"Software de Gestión de Incidentes"*, para su reparación o cambio por garantía (si se encuentra en cobertura); así mismo, queda terminantemente prohibido la manipulación del equipo por parte de personal no autorizado.

6.5.5 Existen los siguientes **Niveles** de Servicio de Telefonía IP:

Nivel 0: Anexo interno.

Nivel 1: Anexo interno y Fijo Local.

Nivel 2: Anexo interno, Fijo Local y Fijo Nacional.

Nivel 3: Anexo interno, Fijo Local, Fijo Nacional y Móvil.

Nivel 4: Anexo interno, Fijo Local, Fijo Nacional, Móvil e Internacional.

El **Nivel 0** es asignado automáticamente al momento de la instalación del Teléfono IP.

6.5.6 Los niveles de servicio de telefonía IP son habilitados mediante una clave de llamada asignado por la Sub Gerencia de Operaciones Telemáticas.

6.5.7 El nivel de llamada asignado al usuario es para uso estrictamente laboral, siendo responsable por todas las llamadas que se generen haciendo uso del código de acceso asignado; para tal efecto, el servidor civil debe asegurar la confidencialidad del código de acceso asignado.

6.5.8 El permiso del **Nivel 4** se habilita por un máximo de 30 días para aquellos usuarios que, por la naturaleza de sus actividades, requieran de este nivel de servicio.

6.5.9 Cuando se detecte que un usuario utiliza un código de acceso de telefonía IP que no le pertenece, los analistas a cargo del servicio de telefonía IP de la Sub Gerencia de Operaciones Telemáticas emiten un informe técnico a la GTI con copia a la GTH informando del hecho para su evaluación y acciones pertinentes.

6.5.10 La Sub Gerencia de Operaciones Telemáticas está facultada para suspender el servicio de telefonía IP asignado al usuario, cuando su uso no está relacionado con las labores asignadas propósitos institucionales. Así mismo, si el usuario no lo utiliza por más de 90 días, se suprime o reasigna el servicio de telefonía IP.

6.6 DEL SERVICIO DE INFRAESTRUCTURA DE COMUNICACIÓN

6.6.1 La Sub Gerencia de Operaciones Telemáticas es la unidad orgánica responsable de realizar los diseños y supervisión de los sistemas de cableado estructurado en todas las sedes del RENIEC a nivel nacional. Así como las coordinaciones y acciones que sean necesarias para asegurar la continuidad y operatividad del mismo, en función a los recursos y capacidades disponibles.

6.6.2 Para realizar cambios, traslados o modificaciones dentro de los ambientes de trabajo que involucren instalación, reubicación o habilitación de nuevos puntos de red, los titulares de las áreas (Gerentes, Jefes de Oficinas, Sub Gerentes, Jefes Regionales, Administradores de Agencias, Jefes de las Oficinas Registrales de RENIEC y Jefes de Oficinas de la Entidad de Registro del Estado Peruano - EREP) deben coordinar con la Sub Gerencia de Operaciones Telemáticas la evaluación de la factibilidad de los cambios solicitados para prevenir la interrupción de los servicios que pueda repercutir en las labores diarias y en la atención al público.

6.6.3 Se debe reportar a la Sub Gerencia de Operaciones Telemáticas, mediante el "Software de Gestión de Incidentes", cualquier falla/avería presentada en el funcionamiento de la red para proceder con la verificación y evaluación del incidente presentado.

6.6.4 Está prohibido que los usuarios realicen reubicaciones o instalaciones de equipos de red (computadoras, Teléfonos IP, impresoras, equipos móviles, periféricos, etc.) a puntos de datos existentes, bajo responsabilidad del Jefe del área.

6.6.5 Es responsabilidad del área otorgar las facilidades y autorizaciones de ingreso para la instalación y configuración de equipos de red (computadoras, Teléfonos IP, impresoras, equipos móviles, periféricos, etc.); de no darse el caso, el requerimiento no es atendido.

6.7 DEL SERVICIO DE VIDEOCONFERENCIA

6.7.1 La Sub Gerencia de Operaciones Telemáticas es la encargada de la administración del servicio de videoconferencia en el RENIEC.

6.7.2 Las áreas del RENIEC que por necesidad del servicio requieran la adquisición de un nuevo equipo de videoconferencia, deben coordinar con la Sub Gerencia de Operaciones Telemáticas la elaboración de las Especificaciones Técnicas (EETT) correspondientes para dar inicio al proceso de adquisición del equipo requerido.

6.7.3 En caso de falla/avería en el funcionamiento del equipo de videoconferencia, se debe reportar a Mesa de Ayuda o a través del "Software de Gestión de Incidentes", para proceder con la verificación de la operatividad y evaluación del incidente presentado.

6.7.4 Es responsabilidad del área usuaria la interrupción del funcionamiento u operatividad del equipo de videoconferencia si éste se traslada a otro ambiente sin previa coordinación ni autorización de la SGOT.

6.7.5 La información expuesta durante la transmisión de una videoconferencia es responsabilidad del organizador; así como la grabación, reproducción y/o transmisión del contenido de las sesiones por otros medios.

6.7.6 Las grabaciones solicitadas por los usuarios del servicio de videoconferencia se almacena en los servidores correspondientes hasta un período máximo de tres (03) días útiles; pasado el plazo se procede a eliminar la grabación.

6.8 DEL SERVICIO VPN (RED PRIVADA VIRTUAL)

6.8.1 La Sub Gerencia de Operaciones Telemáticas es la unidad orgánica encargada de la administración del servicio VPN, monitorea el uso de este servicio y toma las acciones necesarias para asegurar la confiabilidad del mismo, en función a los recursos y capacidades disponibles.

6.8.2 El acceso a los recursos de la red interna del RENIEC mediante una conexión VPN, a través de la red pública internet, es un servicio que brinda la GTI a los usuarios autorizados por las distintas áreas, para el desarrollo de las actividades y responsabilidades asignadas en su entorno laboral.

6.8.3 El servicio VPN está priorizado para ser utilizado por los funcionarios de la institución con nivel de: Gerente, Jefe de Oficina, Sub Gerente y Jefe Regional; así como los servidores civiles que administran servicios tecnológicos críticos dentro de la GTI, de manera que se les permita contribuir con el desarrollo y cumplimiento de las actividades, funciones u objetivos institucionales.

6.8.4 El área responsable de las Agencias u Oficinas Registrales Auxiliares ubicadas en lugares remotos, que cuenten con acceso a internet, puede solicitar el servicio VPN para el registrador en dicho punto de atención de manera temporal. La Sub Gerencia de Operaciones Telemáticas procede con la atención de la solicitud conforme lo estipulado en la Directiva DI-335-GTI/001 "Conexión de la Red del Registro Nacional de Identificación y Estado Civil – RENIEC" (numerales 6.3 y 7.3).

6.8.5 Las credenciales asociadas al servicio VPN, generadas y asignadas a cada usuario autorizado, son personales e intransferibles, bajo responsabilidad.

6.8.6 Los certificados digitales generados por la plataforma VPN se utilizan en los dispositivos móviles institucionales de los funcionarios que cuenten con el servicio VPN para la autenticación al servicio.

6.8.7 Se prohíbe la instalación del software cliente VPN y el uso del servicio VPN en computadoras potencialmente inseguras, como es el caso de las cabinas de internet públicas; pues los referidos ambientes no ofrecen las garantías de confidencialidad de la información requeridas para el uso seguro de este servicio.

6.8.8 El uso del servicio VPN está prohibido para fines ajenos a los dispuestos en la presente directiva.

6.9 DE LA ATENCIÓN PARA LA PUBLICACIÓN DE SERVICIOS Y/O APLICACIONES WEB

DE LA EVALUACIÓN O ANÁLISIS DE VULNERABILIDADES

6.9.1 La Sub Gerencia de Operaciones Telemáticas es la unidad orgánica encargada de la evaluación, publicación en internet y protección de los servicios y/o aplicaciones web, en función a los recursos y capacidades disponibles.

6.9.2 El análisis de vulnerabilidades se realiza a todos los servicios y/o aplicaciones web en el ambiente de producción antes de dar inicio al uso por parte de los usuarios finales. El resultado del análisis se entrega en un reporte resumen con las vulnerabilidades altas y/o críticas encontradas y las recomendaciones para su corrección.

DE LA PUBLICACIÓN A INTERNET DE LOS SERVICIOS Y/O APLICACIONES WEB

6.9.3 Los servicios y/o aplicaciones web se publican en internet cuando las vulnerabilidades altas y/o críticas encontradas hayan sido corregidas por el solicitante.

VII. DISPOSICIONES ESPECÍFICAS

7.1. DEL SERVICIO DE PERFIL DE DOMINIO

DEL ALTA DEL SERVICIO

7.1.1 La solicitud del alta del perfil de dominio para los servidores civiles debe realizarse a través del "Software de Gestión de Incidentes" adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios (Perfil de Dominio, Correo Electrónico, Messenger Interno, Internet y Telefonía IP)" - Anexo N° 02, firmado digitalmente por el Gerente, Jefe de Oficina, Sub Gerente y/o Jefe Regional, indicando lo siguiente:

a. Nombre completo y DNI del servidor civil para quien se solicita la habilitación de perfil de dominio.

b. Para el perfil opcional se sugiere la inicial del nombre a utilizarse seguido del apellido.

   Por ejemplo: El Sr. Juan Pablo Flores Mendoza, puede poseer la cuenta con la inicial de su primer nombre: Jflores o la inicial de su segundo nombre: Pflores (se escoge solo una alternativa). Si al efectuar las combinaciones anteriores se determina la existencia de una cuenta similar, se añaden progresivamente las letras del apellido materno hasta conseguir una cuenta no repetida.

c. Función que desempeña, área a la cual pertenece, ubicación física (sede o local) del usuario, turno y modalidad de contrato.

7.1.2 La Sub Gerencia de Operaciones Telemáticas, una vez recibido el requerimiento, activa la cuenta de usuario de dominio, asigna el nombre del usuario sugerido en el formato y la contraseña correspondiente. La contraseña solo está vigente hasta el primer inicio de sesión del usuario, después de lo cual el sistema solicita el ingreso de una nueva contraseña.

7.1.3 La configuración del perfil de dominio en la computadora asignada al servidor civil, es realizada directamente por personal de la Sub Gerencia de Soporte Técnico Operativo, quienes configuran el nombre de la cuenta de usuario como el nombre de la computadora, de acuerdo a la política establecida, a fin de facilitar la identificación del usuario. Las computadoras que son utilizadas por más de una persona, el nombre (hostname) de la computadora es asignado por la Sub Gerencia de Operaciones Telemáticas.

7.1.4 Para la asignación del nombre de la computadora (hostname) se debe tomar en consideración el Anexo N° 01 "Consideraciones para la asignación del nombre del equipo Hostname en el Directorio Activo"

7.1.5 Si por necesidad del servicio el usuario requiere iniciar sesión en una computadora (host) adicional o un equipo distinto al equipo por defecto, el Jefe del área debe solicitar el permiso, especificando el nombre del equipo o la dirección IP.

DE LA BAJA DEL SERVICIO

7.1.6 La baja del servicio de perfil de dominio de un servidor civil se debe solicitar dentro de las 48 horas de haber concluido el vínculo laboral

con la institución, a través del "Software de Gestión de Incidentes", adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios" - Anexo N° 02, firmado digitalmente por el Jefe inmediato, a fin de salvaguardar la información de la institución, indicando lo siguiente:

a. Nombre y DNI de la persona a quien se da la baja.

b. Indicar si es suspensión temporal o baja de la institución.

DE LA SUSPENSIÓN TEMPORAL y ROTACIÓN DEL SERVICIO

7.1.7 Cuando un servidor civil se ausente temporalmente del área, para hacer uso de su período de descanso físico (vacaciones), el Jefe inmediato debe tramitar dentro de las 48 horas de anticipación la suspensión temporal el servicio de perfil de dominio, así mismo cuando se ausente por descanso médico y otros debe comunicar en un plazo no mayor a dos días hábiles a través del "Software de Gestión de Incidentes", adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios" - Anexo N° 02, firmado digitalmente por el Gerente, Jefe de Oficina, Sub Gerente y/o Jefe Regional responsable del servidor civil.

7.1.8 En caso de rotación a una nueva área de un servidor civil autorizado con el servicio de perfil de dominio, el Gerente, Jefe de Oficina, Sub Gerente y/o Jefe Regional responsable debe solicitar la rotación del servicio siguiendo el mismo procedimiento para del alta del servicio, indicando el motivo de dicho cambio.

Bajo ninguna circunstancia está permitido proporcionar o resetear la contraseña del perfil de dominio de un usuario ausente temporalmente del área, para ser utilizada por otro usuario, bajo responsabilidad. Si para las labores operativas se requiere utilizar la computadora del usuario ausente, debe solicitarse el permiso de inicio de sesión en una computadora (host) adicional, cumpliendo la directiva vigente.

7.1.9 Los requerimientos deben realizarse para un máximo de diez usuarios por cada solicitud. En caso que el área tenga requerimientos para más de diez usuarios, debe enviar la primera solicitud con diez usuarios y, una vez que se haya culminado con la atención del requerimiento, debe solicitar la atención de los usuarios restantes en un nuevo requerimiento, siempre considerando un máximo de diez usuarios por solicitud.

7.1.10 El "Formato de Alta, Baja, Suspensión y Rotación de los Servicios" - Anexo N° 02, que se encuentra firmado digitalmente por otro servidor civil que no haya sido designado para esta actividad mediante un documento formal, no se considera válido.

7.1.11 Las áreas que cuenten con Certificaciones ISO deben realizar sus requerimientos a través del "Software de Gestión de Incidentes", adjuntando "Formato de Alta, Baja, Suspensión y Rotación de los Servicios" - Anexo N° 02, firmado digitalmente por el Gerente o Sub Gerente del área correspondiente. Estos requerimientos se atienden de manera prioritaria dando cumplimiento al Acuerdo de Partes.

7.1.12 Los servicios de comunicación de Alta, Baja, Suspensión y Rotación para los funcionarios de Jefatura Nacional, Alta Dirección y Gerentes,

se tramitan mediante el envío del acto resolutivo por el Sistema Integrado de Trámite Documentario.

7.2 DEL SERVICIO DE CORREO ELECTRÓNICO

DEL ALTA DEL SERVICIO

7.2.1 La solicitud de alta del correo electrónico para un servidor civil debe realizarse a través del "Software de Gestión de Incidentes", adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios" - Anexo N° 02, firmado digitalmente por el Gerente y/o Jefe de Oficina del área al que pertenece.

a. Debe precisarse en el formato, los ***niveles de permisos*** del correo electrónico, de acuerdo a lo siguiente:

1. **Correo electrónico para uso interno**: No se puede enviar ni recibir mensajes fuera de RENIEC.
2. **Envío y recepción de Correos Electrónicos no gratuitos:** Se reciben mensajes provenientes de cualquier dominio, excepto de los dominios gratuitos).

b. Si se requiere incluir la cuenta en un ***grupo de distribución*** se debe proceder de acuerdo a los siguientes casos:

1. Si la cuenta de usuario creada requiere ser incluida en un Grupo de distribución existente, se debe indicar el nombre del grupo en el campo ***"Nombre de Grupo"***.
2. Si la cuenta de usuario creada requiere un nuevo Grupo de distribución sugerir el nombre del grupo en el campo ***"Nuevo Grupo"***.

7.2.2 La Sub Gerencia de Operaciones Telemáticas crea el buzón correspondiente el cual es configurado en el cliente Outlook instalado en la computadora del usuario por el personal de la Sub Gerencia de Soporte Técnico Operativo.

7.2.3 Los Grupos de Distribución sólo se crean cuando su alcance sea de interés institucional. Para solicitar la creación de éste grupo, debe consignarse el nombre sugerido del grupo de distribución y en el campo de justificación la lista de integrantes del grupo. Antes de solicitar la creación de un grupo de distribución se debe coordinar con el responsable de la administración del servicio de correo electrónico la asignación del nombre respectivo.

7.2.4 Cuando el usuario requiera la creación del buzón de correo electrónico adicional, se debe solicitar a través del "Software de Gestión de Incidentes", adjuntando el el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios" - Anexo N° 02, firmado digitalmente por el Gerente o Jefe de Oficina solicitante, debiendo consignar en el formato:

a. Nombre del administrador responsable en el campo DATOS DEL USUARIO.

b. Marcar en el formato de Buzón Adicional y colocar el nombre sugerido del buzón.

c. En el campo JUSTIFICACIÓN consignar la lista de los usuarios con acceso al buzón adicional.

d. El alta o baja de usuarios con acceso al buzón adicional debe solicitarse mediante el mismo procedimiento. El administrador del buzón es responsable de trasladar periódicamente los mensajes del buzón a una carpeta personal.

DEL INGRESO DE CORREOS ELECTRÓNICOS PROVENIENTES DE SERVIDORES GRATUITOS

7.2.5 Para aquellas áreas en las que, adicionalmente a los permisos existentes, requiera que el servidor civil reciba o envíe correos electrónicos gratuitos en el buzón de RENIEC, el Gerente y/o Jefe de Oficina del área debe solicitar la autorización mediante un memorando a la GTI, sustentando debidamente la necesidad por cada usuario y haciendo mención específica del "permiso para recepción y envío de mensajes de correo electrónico provenientes y destinados desde y hacia servidores gratuitos". El memorando es derivado a la Sub Gerencia de Operaciones Telemáticas para su evaluación y autorización en caso corresponda. Éste permiso puede otorgarse con posterioridad a la habilitación del servicio.

DE LA BAJA DEL SERVICIO

7.2.6 Cuando un servidor civil culmine su vínculo laboral con la Institución, el Jefe inmediato debe tramitar dentro de las 48 horas la baja de servicio de correo electrónico a través del "Software de Gestión de Incidentes", adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios" - Anexo N° 02, firmado digitalmente por el Gerente, Jefe de Oficina, Sub Gerente y/o Jefe Regional.

DE LA SUSPENSIÓN TEMPORAL y ROTACIÓN DEL SERVICIO

7.2.7 Cuando un servidor civil se ausente temporalmente del centro de labores, para hacer uso de su período de descanso físico (vacaciones), el Jefe inmediato debe tramitar dentro de las 48 horas de anticipación la suspensión temporal del servicio de correo electrónico, así mismo cuando se ausente por descanso médico y otros debe comunicar en un plazo no mayor a 48 horas hábiles a través del "Software de Gestión de Incidentes", adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios" - Anexo N° 02, firmado digitalmente por el Gerente, Jefe de Oficina, Sub Gerente y/o Jefe Regional responsable del servidor civil.

7.2.8 En caso de rotación a una nueva área de un servidor civil autorizado con el servicio de correo electrónico el Gerente, Jefe de Oficina, Sub Gerente, o Jefe Regional responsable debe solicitar la desactivación del servicio siguiendo el mismo procedimiento para la activación, indicando el motivo de dicho cambio.

7.2.9 Para la solicitud de los requerimientos se debe tomar en cuenta los numerales 7.1.9. y 7.1.10

7.2.10 Las unidades orgánicas con certificaciones ISO realizan sus requerimientos de acuerdo al numeral 7.1.11.

7.2.11 Las solicitudes servicios de comunicación de Alta, Baja, Suspensión y Rotación para los funcionarios de Jefatura Nacional, Alta Dirección y Gerentes se tramitan de acuerdo al numeral 7.1.12.

7.3 DEL SERVICIO DE MENSAJERÍA (MESSENGER INTERNO)

DEL ALTA DEL SERVICIO

7.3.1 La solicitud de alta de mensajería (Messenger Interno) para un servidor civil se debe realizar a través del "Software de Gestión de Incidentes", adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicio" - Anexo N° 02, firmado digitalmente por el Gerente de la unidad orgánica correspondiente.

7.3.2 La Sub Gerencia de Operaciones Telemáticas, previa evaluación de la solicitud de requerimiento procede a habilitar el servicio, el cual es configurado en la computadora del usuario por la Sub Gerencia de Soporte Técnico Operativo.

DE LA BAJA DEL SERVICIO

7.3.3 La baja del servicio de mensajería de un servidor civil debe ser solicitado por el Gerente, Jefe de Oficina, Sub Gerencia o Jefatura Regional siguiendo el mismo procedimiento para la alta del servicio.

7.3.4 Para la solicitud de los requerimientos se debe tomar en cuenta los numerales 7.1.9; 7.1.10; y 7.1.12.

7.4 DEL SERVICIO DE INTERNET

DE LOS NIVELES DE ACCESO EXISTENTES

7.4.1 **Personalizado:** Nivel que permite al usuario acceder sólo a páginas web específicas o a un cierto dominio. Ejemplo: páginas de gobierno (*.gob.pe), páginas de dominio org (*.org y *.org.pe), páginas amarillas y páginas blancas, entre otras. Este nivel de acceso está dirigido al servidor civil que solo requieren el acceso a páginas de internet o dominios específicos, mayormente gubernamentales o de instituciones del estado.

7.4.2 **Básico:** Nivel que permite al usuario acceder a cualquier página web cuyo contenido no esté prohibido ni restringido por las políticas establecidas para el servicio de internet (acápite 6.4 de la presente Directiva). Incluye permisos para la descarga de archivos únicamente de los siguientes tipos: *.doc, *.xls, *.ppt y *.pdf. Adicionalmente puede descargar archivos comprimidos (*.zip) pero sólo de páginas de gobierno (*.gob.pe). Este nivel de acceso está dirigido a todos los usuarios de la institución que requieran de acceso a internet para el desarrollo normal de sus funciones

7.4.3 **Intermedio:** Nivel que permite al usuario, además de contar con los permisos del "Nivel Básico", el acceso a páginas con contenido multimedia; estos accesos a contenido multimedia debe ser autorizado y justificado por el área responsable del usuario en el formato de solicitud del servicio. Se aplica sólo a los servidores civiles que cumple funciones de comunicación, relaciones públicas, prensa, protocolo e investigación; que por la naturaleza especial de sus funciones y actividades deben interactuar con contenidos multimedia. Para el acceso a los servicios de almacenamiento en la nube, Redes Sociales o a Mensajería Instantánea Externa, el área responsable del usuario debe solicitarlos con un memorando dirigido a la GTI, justificando la necesidad y detallando las páginas y/o

aplicaciones específicas que se deben habilitar a sus usuarios autorizados.

7.4.4 **Soporte:** Nivel que permite al usuario, además de contar con los permisos del "Nivel Básico", la descarga de archivos especiales tales como drivers, instaladores, archivos ejecutables y archivos comprimidos. Este nivel se otorga sólo a los servidores civiles de la GTI que brinda labores de soporte técnico, desarrollo de software, gestión de base de datos y operaciones telemáticas. Si adicionalmente requieren accesos a páginas de contenido multimedia, servicios de acceso remoto, servicios de almacenamiento en la nube, Redes Sociales o Mensajería Instantánea Externa deben estar autorizados por el Sub Gerente responsable del usuario y solicitados a través del "Software de Gestión de Incidentes", justificando la necesidad y detallando las páginas y/o aplicaciones específicas que se deben habilitar.

7.4.5 **Funcionario:** Nivel especial con acceso a contenido multimedia, servicios de almacenamiento en la nube, redes sociales y/o mensajería instantánea externa. Aplicable sólo para funcionarios con niveles de gerente, jefe de oficina, sub gerente y jefe regional.

DEL ALTA DEL SERVICIO

7.4.6 La solicitud de alta de internet para el servidor civil debe ser realizada a través del "Software de Gestión de Incidentes", adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios" - Anexo N° 02 firmado digitalmente por el Gerente y/o Jefe de Oficina del área al que pertenece, indicando:

a. Usuario.

b. Nivel de Acceso.

c. Justificación del Nivel de Acceso solicitado.

7.4.7 En caso existan facilidades y/o las capacidades del servicio de internet lo permitan, se procede a habilitar el servicio respectivo para el servidor civil.

DE LA BAJA DEL SERVICIO

7.4.8 El Jefe inmediato tramita, dentro de las 48 horas de producido el hecho, la baja del servicio de internet cuando un servidor civil culmina su vínculo laboral con la institución; para tal efecto, se hace uso del "Software de Gestión de Incidentes" adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios" - Anexo N° 02, firmado digitalmente por el Gerente, Jefe de Oficina, Sub Gerente y/o Jefe Regional responsable del usuario.

DE LA SUSPENSIÓN TEMPORAL y ROTACIÓN DEL SERVICIO

7.4.9 Cuando un servidor civil se ausente temporalmente del centro de labores, para hacer uso de su período de descanso físico (vacaciones), el Jefe inmediato debe tramitar dentro de las 48 horas de anticipación la suspensión temporal el servicio de internet, así mismo cuando se ausente por descanso médico u otros, debe comunicar en un plazo no mayor a dos (02) días hábiles a través del "Software de Gestión de Incidentes", adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios" - Anexo N° 02 firmado

digitalmente por el Gerente, Jefe de Oficina, Sub Gerente y/o Jefe Regional responsable del servidor civil.

7.4.10 En caso de rotación a una nueva área de un servidor civil autorizado con el servicio de internet el Gerente, Jefe de Oficina, Sub Gerente y/o Jefe Regional responsable debe solicitar la rotación del servicio siguiendo el mismo procedimiento para el alta del servicio, indicando el motivo de dicho cambio.

7.4.11 Para la solicitud de los requerimientos se debe tomar en cuenta los numerales 7.1.9 y 7.1.10.

7.4.12 Las unidades orgánicas con certificaciones ISO realizan sus requerimientos de acuerdo al numeral 7.1.11.

7.4.13 Las solicitudes servicios de comunicación de Alta, Baja, Suspensión y Rotación para los funcionarios de Jefatura Nacional, Alta Dirección y Gerentes se tramitan de acuerdo al numeral 7.1.12.

7.5 DEL SERVICIO DE TELEFONÍA IP

DEL LA INSTALACIÓN DE TELÉFONO IP

7.5.1 La solicitud de instalación del servicio de telefonía IP para un usuario debe ser realizada a través de Mesa de Ayuda o por el "Software de Gestión de Incidentes", adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios"- Anexo N° 02 firmado digitalmente por el Gerente y/o Jefe de Oficina del área correspondiente.

7.5.2 La Sub Gerencia de Operaciones Telemáticas, una vez recibido el requerimiento, dispone realizar una visita de inspección a fin de determinar la factibilidad de la solicitud y en caso se cuente con todos los recursos (equipo y punto de red), se procede con la instalación respectiva, en caso contrario se comunica al área solicitante.

DE LA REUBICACIÓN DE TELÉFONO IP

7.5.3 La solicitud de reubicación del teléfono IP debe ser realizada a través de Mesa de Ayuda o por el "Software de Gestión de Incidentes", adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios" - Anexo N° 02 firmado digitalmente por el Gerente y/o Jefe de Oficina del área correspondiente.

La reubicación del teléfono IP se realiza siempre y cuando exista un punto de red disponible.

DE LA TRANSFERENCIA DE NÚMERO DE ANEXO EXISTENTE

7.5.4 La solicitud de transferencia de número de anexo existente para un usuario debe ser realizada a través de Mesa de Ayuda o por el "Software de Gestión de Incidentes", adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios"- Anexo N° 02 firmado digitalmente por el gerente y/o jefe de oficina del área correspondiente.

DE LA ASIGNACIÓN DE NÚMERO DE ANEXO

7.5.5 La asignación de número de anexo debe ser realizada o a través de Mesa de Ayuda o por el "Software de Gestión de Incidentes", adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios" - Anexo N° 02 firmado digitalmente por el Gerente y/o Jefe de Oficina del área correspondiente.

Para atención de la asignación del número de anexo para un servidor civil se requiere contar con un equipo de telefonía IP, de no ser así el requerimiento no es atendido.

DEL CAMBIO DE CLAVE DE LLAMADA

7.5.6 La solicitud de cambio de clave de llamada debe ser realizada a través de Mesa de Ayuda o por el "Software de Gestión de Incidentes", adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios - Anexo N° 02 firmado digitalmente por el Gerente y/o Jefe de Oficina del área correspondiente.

7.5.7 Para el caso de cambio de unidad orgánica o dependencia del servidor civil se debe indicar el nivel de servicio en el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios"- Anexo N° 02 firmado digitalmente por el Gerente y/o Jefe de Oficina del área correspondiente.

DEL CAMBIO DE NIVEL DE SERVICIO

7.5.8 La solicitud de cambio de nivel de servicio de telefonía IP para un usuario debe ser realizada a través de Mesa de Ayuda o por el "Software de Gestión de Incidentes", adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios" - Anexo N° 02 firmado digitalmente por el Gerente y/o Jefe de Oficina del área correspondiente, indicando la clase de servicio:

Nivel de servicio
1 Anexo Interno y Fijo Local
2 Anexo Interno, Fijo Local y Fijo Nacional
3 Anexo Interno, Fijo Local, Fijo Nacional y Móvil
4 Anexo Interno, Fijo Local, Fijo Nacional, Móvil e Internacional

DE LA BAJA DE CLAVE DE LLAMADA

7.5.9 La solicitud de baja de clave de llamada debe ser realizada a través de Mesa de Ayuda o por el "Software de Gestión de Incidentes", adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios" - Anexo N° 02 firmado digitalmente por el Gerente y/o Jefe de Oficina del área correspondiente.

DE LA BAJA DE SERVICIO

7.5.10 El Jefe inmediato tramita, dentro de las 48 horas de producido el hecho, la baja del servicio de internet cuando un servidor civil culmina su vínculo laboral con la institución; para tal efecto, se hace uso del "Software de Gestión de Incidentes" adjuntando el "Formato de Alta, Baja, Suspensión y Rotación de los Servicios" - Anexo N°

02, firmado digitalmente por el Gerente, Jefe de Oficina, Sub Gerente y/o Jefe Regional responsable del usuario

7.5.11 Para la solicitud de los requerimientos se debe tomar en cuenta los numerales 7.1.9 y 7.1.10.

7.5.12 Las unidades orgánicas con certificaciones ISO realizan sus requerimientos de acuerdo al numeral 7.1.11.

7.5.13 Las solicitudes servicios de comunicación de Alta, Baja, Suspensión y Rotación para los funcionarios de Jefatura Nacional, Alta Dirección y Gerentes se tramitan de acuerdo al numeral 7.1.12.

7.6 DEL SERVICIO DE INFRAESTRUCTURA DE COMUNICACIÓN DE LA INSTALACIÓN DEL PUNTO DE RED

7.6.1 La solicitud de la instalación, habilitación y reubicación de puntos de red en un local debe ser realizada a través del "Software de Gestión de Incidentes", adjuntando el "Formato del Servicio de Infraestructura de Comunicación (Instalación, Habilitación y Reubicación de Punto de Red)" - Anexo N° 03 firmado digitalmente por el Jefe inmediato del área correspondiente; asimismo, debe incluir el plano de distribución de los equipos de cómputo y periféricos en el que se indique la ubicación de los puntos de red.

7.6.2 La solicitud de instalación o habilitación de más de cinco de puntos de red por remodelación y/o ampliación de un local y/o ambiente existente o nuevo debe ser realizado por el Gerente, Jefe de Oficina, Sub Gerente, Jefe Regional o Jefe de Oficina Registral correspondiente, mediante un memorando a la GTI adjuntando el "Formato del Servicio de Infraestructura de Comunicación"- Anexo N° 03 firmado digitalmente por el solicitante y el plano de distribución de los equipos de cómputo y periféricos en el que se indique la ubicación de los puntos de red.

7.6.3 La Sub Gerencia de Operaciones Telemáticas una vez recibido el requerimiento de instalación o habilitación de puntos de red en un local y/o ambiente nuevo, dispone realizar una visita de inspección a fin de determinar la factibilidad de la solicitud. De ser factible se procede a elaborar la relación de materiales o las Especificaciones Técnicas de ser el caso.

7.6.4 Los trabajos de instalación de puntos de red se realizan una vez que se disponga con todos los materiales requeridos, de acuerdo al plano de distribución proporcionado por el solicitante.

7.6.5 La solicitud de verificación de puntos de red debe ser realizada a través del "Software de Gestión de Incidentes" o Mesa de Ayuda.

7.6.6 La conformidad del servicio informático a los trabajos de implementación realizados por terceros, es efectuado por el área usuaria y un especialista de la Sub Gerencia de Operaciones Telemáticas y/o el asistente informático.

7.6.7 Los cambios de locales deben ser coordinados con la Sub Gerencia de Operaciones Telemáticas para la evaluación y planificación respectiva.

7.6.8 Para la solicitud de los requerimientos se debe tomar en cuenta el los numerales 7.1.9. y 7.1.10.

7.7 DEL SERVICIO DE VIDEOCONFERENCIA

DE LA ACTIVACIÓN DEL SERVICIO

7.7.1 La solicitud del servicio de videoconferencia debe ser realizada a través de Mesa de Ayuda o por el "Software de Gestión de Incidentes", adjuntando el "Formato del Servicio de Videoconferencia (Programación, nueva instalación, reubicación y/o configuración – Soporte)" - Anexo N° 04, firmado digitalmente por el Gerente, Jefe de Oficina, Sub Gerente y/o Jefe Regional.

7.7.2 Una vez recibido la solicitud, la Sub Gerencia de Operaciones Telemáticas, procede a disponer la atención del servicio solicitado. No se acepta la solicitud cuando los equipos de videoconferencia están siendo utilizados en otra sesión.

7.7.3 La solicitud de programación del servicio de videoconferencia interna debe ser solicitada con **48 horas de anticipación**; debiéndose registrar en el formato la fecha, hora y los contactos del área.

7.7.4 La solicitud de programación del servicio de videoconferencia externa debe ser realizada **con cinco días hábiles de anticipación**; debiéndose registrar obligatoriamente en el formato la fecha, hora, los contactos de las áreas y externos.

DE LA CANCELACIÓN DEL SERVICIO

7.7.5 El servicio de videoconferencia se cancela cuando no cumpla con los objetivos, políticas y fines generales de este servicio o se atente contra la integridad de las personas y/o violente el régimen jurídico del RENIEC.

DEL SOPORTE DEL SERVICIO DE VIDEOCONFERENCIA

7.7.6 La solicitud de la instalación, reubicación física del equipo de videoconferencia debe ser solicitada con una antelación de cinco días útiles a través de Mesa de Ayuda o en el "Software de Gestión de Incidentes", adjuntando el "Formato del Servicio de Videoconferencia" - Anexo N° 04, firmado digitalmente por el Gerente, Jefe de Oficina, Sub Gerente y/o Jefe Regional.

7.7.7 La solicitud de configuración del equipo de videoconferencia por cambio en la estructura orgánica en el Reglamento de Organización y Funciones (ROF) se debe realizar a través de Mesa de Ayuda o en el "Software de Gestión de Incidentes", adjuntando el "Formato del Servicio de Videoconferencia" - Anexo N° 04, firmado digitalmente por el Gerente, Jefe de Oficina, Sub Gerente y/o Jefe Regional.

7.7.8 Una vez recibida la solicitud de "Programación, nueva instalación, reubicación y/o configuración- Soporte" del servicio de videoconferencia, la Sub Gerencia de Operaciones Telemáticas procede a disponer la atención del servicio solicitado. No se acepta la solicitud cuando el(los) equipo(s) de videoconferencia está(n) siendo utilizado(s) en otra sesión.

7.7.9 La solicitud del requerimiento de elaboración de especificaciones técnicas del equipo de videoconferencia debe realizarse a través de Mesa de Ayuda o por el "Software de Gestión de Incidentes", adjuntando el "Formato del Servicio de Videoconferencia" - Anexo N° 04, firmado digitalmente por el Gerente, Jefe de Oficina, Sub Gerente y/o Jefe Regional.

7.7.10 Una vez recibido el requerimiento de elaboración de las especificaciones técnicas del equipo de videoconferencia, la Sub Gerencia de Operaciones Telemáticas procede a disponer la atención del requerimiento de acuerdo a la disponibilidad de los servidores civiles para la elaboración de las especificaciones técnicas.

7.7.11 El "Formato del Servicio de Videoconferencia (programación, nueva instalación, reubicación y/o configuración- soporte)" - Anexo N° 04, que se encuentra firmado digitalmente por otro servidor civil que no haya sido designado para esta actividad mediante un documento formal, no se considera válido.

7.8 DEL SERVICIO VPN

DE LOS PERFILES DE USUARIOS Y SUS ACCESOS

7.8.1 **Perfil Funcionario:** Los funcionarios con niveles de Gerente, Jefe de Oficina, Sub Gerente y Jefe Regional, tienen acceso al servicio de correo, trámite documentario, intranet y acceso remoto a su computadora. El usuario VPN de un Funcionario se mantiene vigente, mientras tenga permanencia en su respectivo cargo.

7.8.2 **Perfil Administrador de Servicio Crítico:** Los servidores civiles de la GTI que administran los servicios tecnológicos críticos, tienen acceso al servicio de correo, acceso remoto a su computadora y a los servidores bajo su administración. El usuario VPN de un Administrador de Servicio Crítico tiene un periodo de validez de 180 días (06 meses), a partir del cual el área responsable del usuario tiene que solicitar su renovación. Se exceptúa del periodo de validez a los administradores de seguridad informática y administradores de redes de la Sub Gerencia de Operaciones Telemáticas, quienes por la naturaleza de sus funciones necesitan del servicio VPN por un periodo indefinido.

7.8.3 **Perfil Registrador:** El personal asignado al registro de ciudadanos en una agencia remota, tiene acceso a las aplicaciones internas que correspondan a las funciones asignadas por su área en el horario laboral solicitado, fuera de este horario el servicio está inactivo por seguridad. El usuario VPN de un Registrador tiene un periodo de validez de 365 días (12 meses), a partir del cual el área responsable del usuario debe solicitar su renovación

DEL ALTA DEL SERVICIO

7.8.4 La solicitud de alta del servicio VPN para un usuario debe ser realizada a través del "Software de Gestión de Incidentes", adjuntando el "Formato del Servicio VPN (Alta, Renovación y Baja del servicio)"- Anexo N° 05, firmado digitalmente por el Gerente y/o Jefe de Oficina del área correspondiente, indicando:

a. ***Para el perfil de Administrador de Servicio Crítico*:**

Periodo (no mayor a 180 días).

b. ***Para el perfil registrador:***

Periodo (no mayor a 365 días).

Horario laboral (registro obligatorio).

Acceso a los sistemas.

Adicionalmente se debe adjuntar el "Acta de confidencialidad del Servicio VPN" (Anexo N° 06), firmado por el usuario final, como un compromiso para resguardar la seguridad de la información del RENIEC y cumplir con todas las políticas descritas en la presente directiva.

7.8.5 Para el caso de los administradores de seguridad informática y administradores de redes de la Sub Gerencia de Operaciones Telemáticas, el líder responsable de cada área debe remitir por correo electrónico el alta de los usuarios VPN de los administradores bajo su responsabilidad, adjuntando el "Acta de Confidencialidad del Servicio VPN".

7.8.6 De contar con los recursos informáticos necesarios y disponibles, la Sub Gerencia de Operaciones Telemáticas procede a configurar los accesos y en coordinación con el área solicitante se realiza la instalación del software cliente VPN en el dispositivo correspondiente.

DE LA RENOVACIÓN DEL SERVICIO

7.8.7 La renovación del servicio VPN debe ser requerido antes que concluya el periodo de validez solicitado a través del "Software de Gestión de Incidentes", adjuntando el ""Formato del Servicio VPN" (Anexo N° 05), firmado digitalmente por el Gerente y/o Jefe de la Oficina del área correspondiente. Se debe indicar el periodo de validez de la renovación del servicio, de acuerdo al perfil correspondiente. En caso no se reciba ninguna solicitud de renovación se procede con la desactivación del servicio y su posterior baja.

DE LA BAJA DEL SERVICIO

7.8.8 Se da la baja cuando el registrador es removido de su función y es reemplazado por otro personal. El área responsable está en la obligación de solicitar la baja del servicio para el registrador anterior y solicitar el alta del servicio para el nuevo registrador, bajo responsabilidad.

7.8.9 La baja del servicio VPN se solicita a través del "Software de Gestión de Incidentes", adjuntando el "Formato del Servicio VPN" (Anexo N° 05), firmado digitalmente por el Gerente y/o Jefe del área correspondiente.

7.8.10 Cuando se recibe una notificación de baja del servidor civil de la institución, por parte de la GTH, que corresponda a un usuario que cuenta con acceso al servicio VPN; se procede a efectuar la baja del servicio para el usuario en mención.

7.8.11 Se desactiva temporalmente el servicio VPN cuando la cuenta no se utiliza por un periodo de sesenta (60) días consecutivos y se notifica al área usuaria para la solicitud de la baja correspondiente.

7.8.12 Para el caso de los administradores de seguridad informática y administradores de redes de la Sub Gerencia de Operaciones Telemáticas, el líder responsable de cada área debe remitir por correo electrónico la desactivación o la baja de los usuarios VPN bajo su responsabilidad.

7.8.13 El "Formato del Servicio VPN (Alta, Renovación y Baja del servicio)"- Anexo N° 05, que se encuentra firmado digitalmente por otro servidor civil que no haya sido designado para esta actividad mediante un documento formal, no se considera válido.

7.9 DE LA ATENCIÓN PARA LA PUBLICACIÓN DE SERVICIOS Y/O APLICACIONES WEB

DE LA SOLICITUD DE ANÁLISIS DE VULNERABILIDADES DE LOS SERVICIOS Y/O APLICACIONES WEB

7.9.1 El líder de proyecto de soporte a la implementación de software solicita el análisis de vulnerabilidades de los servicios y/o aplicaciones web previo a su publicación en internet a través del "Software de Gestión de Incidentes", adjuntando el Formato de "Solicitud de Análisis de Vulnerabilidad de los Servicios y/o Aplicaciones Web" (Anexo N° 07), firmado digitalmente por el Sub Gerente de Ingeniería de Software.

7.9.2 El análisis de vulnerabilidades de los servicios y/o aplicaciones web para la publicación en internet, se ejecuta con herramientas especializadas y recursos disponibles por los analistas de seguridad informática, independientemente en los ambientes de desarrollo y preproducción.

7.9.3 El resultado del análisis de vulnerabilidades de los servicios y/o aplicaciones web es remitido en el Formato de "Reporte de Resultados del Análisis de Vulnerabilidades" (Anexo N° 08), donde se indica la siguiente información:

Resultado de Pruebas de Seguridad		
Factor de Riesgo	**Crítico**	**Alto**
Prioridad	**Alta**	**Media**
Estado	**Atendido**	**Pendiente**

7.9.4 El pase a producción se realiza siguiendo los lineamientos de la NAI 338-GI-001 "Proceso de Gestión de la Configuración".

DE LA SOLICITUD DE PUBLICACIÓN A INTERNET DE LOS SERVICIOS Y/O APLICACIONES WEB

7.9.5 La solicitud de publicación a internet de los servicios y/o aplicaciones web se gestiona siguiendo los lineamientos de la Norma Administrativa Interna NAI 338-GI-001 "Proceso de Gestión de la Configuración" a través del "Software de Gestión de Incidentes", adjuntando el Formato "Solicitud de Publicación a internet de los Servicios y/o Aplicaciones

Web" (Anexo N° 09), firmado digitalmente por el Sub Gerente de Ingeniería de Software.

DE LA SOLICITUD DE BAJA DE LAS PUBLICACIONES A INTERNET DE LOS SERVICIOS Y/O APLICACIONES WEB

7.9.6 La solicitud de baja de las publicaciones a internet de los servicios y/o aplicaciones web debe gestionarse a través del "Software de Gestión de Incidentes", adjuntando el Formato "Solicitud de Publicación a internet de los Servicios y/o Aplicaciones Web" (Anexo N° 09), firmado digitalmente por el Sub Gerente de Ingeniería de Software.

VIII. DISPOSICIONES COMPLEMENTARIAS

La Gerencia de Tecnología de la Información a través de la Sub Gerencia de Operaciones Telemáticas y en coordinación con la Escuela Registral (ER), fomentan 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 N° 01
CONSIDERACIONES PARA LA ASIGNACIÓN DEL NOMBRE DEL EQUIPO HOSTNAME EN EL DIRECTORIO ACTIVO

a. Por defecto el nombre de los equipos de escritorio (hostname) deben coincidir con el nombre de perfil de usuario, excepto cuando el usuario utilice equipos portátiles tales como: Laptops, Tabletas y/o Totems. En estos casos se antepone la nomenclatura LAP, TAB y/o TOTEM. Deben descartarse los nombres de host tipo PC01, ARC05, PRUEBAS2, etc., de encontrarse equipos con estos nombres se deshabilitaran los objetos HOST en el directorio activo.

b. Cuando la computadora sea utilizada por más de un usuario, para la definición del **hostname secundario**, se debe seguir los siguientes pasos:

- Identificar el host principal
- Agregar al host principal la letra inicial del apellido materno.

  Por ejemplo: El usuario José Rivas Mendoza, su ***host principal*** es JRIVAS y el **host secundario** debe ser JRIVASM.
- De existir el host secundario se debe añadir la siguiente letra del apellido materno hasta que se consiga un único host en el directorio activo.

ANEXO N° 02
FORMATO DE ALTA, BAJA, SUSPENSIÓN, ROTACIÓN DE LOS SERVICIOS

FORMATO DE ALTA, BAJA, SUSPENSIÓN y ROTACIÓN DE LOS SERVICIOS

(PERFIL DE DOMINIO, CORREO ELECTRÓNICO, MESSENGER INTERNO, INTERNET y TELEFONÍA IP)

RENIEC — REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

DATOS DEL FORMATO
CODIGO: GC-7.5CT.01SGCT.01RE Versión: 04 Fecha Emisión: 24/08/2012 Fecha Actualización: 24/08/2017

N° Formato: 00001/SGPI/GRI FECHA DE SOLICITUD: 24/08/2017

DATOS DEL SOLICITANTE

GERENCIA/OFICINA:	Gerencia de Registro de Identificación
SUB GERENCIA/JEFATURA REGIONAL	Sub Gerencia de Procesamiento de Identificación
NOMBRES Y APELLIDOS:	Josué Pozo Dionicio

DATOS DEL CONTACTO:

Nombres y Apellidos:	Freddy Olaguibel Mendoza — Teléfono de contacto: 1513

DATOS DEL SERVIDOR CIVIL/ LOCADOR DE SERVICIOS:

Nombres y Apellidos:	Juan Pablo Flores Mendoza — DNI: 24691309
Función:	Analista — Turno: Mañana
Unidad Orgánica:	GRI/SGPI — Modalidad de Contrato: CAS
Ubicación:	Sede Operativa — Piso: 5 — Dirección: Jr. Cusco N° 276
Baja de la institución:	☐

Tipo de Servicio: Perfil de Dominio: ☒ Correo Electrónico: ☐ Telefonía IP: ☐ Messenger Interno: ☐ Internet: ☐

DATOS DEL REQUERIMIENTO

Tipo de Servicio:	Perfil de Dominio	Correo Electrónico	NIVEL ☐
Alta de Servicio	☒	☐	1 Correo para uso interno (no podrá enviar ni recibir
Rotación del usuario y cuenta	☐	☐	2 Envío y recepción de correos no gratuitos (se recibirán y enviarán correos de cualquier dominio, excepto los dominios gratuitos)
Baja de Servicio	☐	☐	
Suspensión temporal del servicio	☐ Del 07/01/2017 Al 31/12/2017	☐ Del Al	
Inicio en PC(host) adicional	☐ Nombre PC / IP: Pflores / 10.50.40.28		
Grupo de Distribución		☐ Nombre de Grupo:	
		☒ Nuevo Grupo: Seguridad	
Buzón Adicional		☐	
Perfil de Usuario Sugerido:	Pflores		
Justificación:			

Importante: Para el caso de que un usuario posea mas de un nombre, se deberá indicar la letra inicial que identificará su cuenta, la misma que puede ser la letra incial de su primer o segundo nombre. Por ejemplo. El Sr. Juan Pablo Flores Mendoza, puede poseer la cuenta con la inicial de su primer nombre: Jflores o segundo nombre: Pflores (escoger solo una alternativa). Si al efectuar las combinaciones anteriores ya existe la cuenta, se añadirán progresivamente las letras del apellido materno hasta conseguir una cuenta no repetida.

Tipo de Servicio:	Messenger Interno	Internet	
Alta de Servicio	☒	☒	NIVEL DE ACCESO INTERNET: 2
Baja de Servicio	☐	☐	1 Personalizado 2 Básico 3 Intermedio 4 Soporte 5 Funcionario
Justificación:			

Tipo de Servicio:	Telefonía IP	Creación de clave de llamada (indicar el nivel del servicio) ☐
Instalación de Teléfono IP	☒	1 Anexo interno y Fijo local
Reubicación de Teléfono IP	☐	2 Anexo interno, Fijo local y Fijo Nacional
Transferencia de número de anexo existente	☐	3 Anexo interno, Fijo local, Fijo Nacional y Móvil
Asignación de número de anexo	☐	4 Anexo interno, Fijo local, Fijo Nacional, Móvil e Internacional
Cambio de clave de llamada	☐	
Baja de Clave de llamada	☐	Cambio de nivel de servicio de ___ a nivel ___ ☐
Baja de Servicio	☐	
Justificación:	Instalación de nuevo anexo telefónico para usuario por necesidad de servicio, en el Piso 7 en SGCO	

SECRETARÍA GENERAL — RENIEC

GERENCIA DE PLANIFICACIÓN Y PRESUPUESTO — RENIEC

SUB GERENCIA DE OPERACIONES TELEMÁTICAS — RENIEC

SUB GERENCIA DE ASESORÍA ADMINISTRATIVA — RENIEC

GERENCIA ASESORÍA JURÍDICA — RENIEC

ANEXO N° 03
FORMATO DEL SERVICIO DE INFRAESTRUCTURA DE COMUNICACIÓN

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

FORMATO DEL SERVICIO DE INFRAESTRUCTURA DE COMUNICACIÓN
(INSTALACIÓN, HABILITACIÓN Y REUBICACIÓN DE PUNTO DE RED)

DATOS DEL FORMATO:
CODIGO: GC-T-F-SIC 02/SGOT/GTYRE Versión: 03 Fecha Emisión: 24/08/2012 Fecha Actualización: 01/02/2017

N° Formato: 00001/SGP/GTH FECHA DE SOLICITUD: 01/02/2017

DATOS DEL SOLICITANTE				
GERENCIA/OFICINA:	Gerencia de Talento Humano			
SUB GERENCIA/JEFATURA REGIONAL:	Sub Gerencia de Desarrollo Humano			
NOMBRES Y APELLIDOS:	Fernando Lopez Villafuerte			
DATOS DEL CONTACTO:				
Nombres y Apellidos:	Karina Diaz Valdivia		**Teléfono de contacto:**	1450
DATOS DEL SERVIDOR CIVIL / LOCADOR DE SERVICIOS:				
Nombres y Apellidos:	Marlene Ortega Auqui		**Turno:**	Mañana
Unidad Orgánica:	GRH/SGDH			
Ubicación:	Sede Administrativa	**Piso:** 29	**Dirección:**	Jr. Bolivia N° 109
Tipo de Solicitud:	**Cableado** [X]		**Instalación de Nueva Agencia:** [ ]	
DATOS DEL REQUERIMIENTO				
Tipo de Solicitud:	**Cableado**			
a) Instalación de punto de red nuevo	[X]			
b) Habilitación de punto de red	[ ]			
c) Reubicación de punto de red	[ ]			
d) Cable de red	[ ]	**Cantidad:** X Unidades	**Longitud:**	Mts.

Nota: *Se debe adjuntar el plano de distribución de PC's en el que se indique la distribución de los puntos de red para los tipos de servico a), b) y c).*

Justificación:

Tipo de Solicitud:	**Instalación de Nueva Unidad Orgánica**
Términos de Referencia	[ ]
Lista de Materiales	[ ]

Justificación:

ANEXO Nº 04
FORMATO SERVICIO DE VIDEOCONFERENCIA

FORMATO DEL SERVICIO DE VIDEOCONFERENCIA
(PROGRAMACIÓN, NUEVA INSTALACIÓN, REUBICACIÓN y/o CONFIGURACIÓN - SOPORTE)

RENIEC

N° Formato: 00001/GOR — FECHA DE SOLICITUD: 01/02/2017

DATOS DEL SOLICITANTE:

GERENCIA:	Gerencia de Operaciones Registrales
SUB GERENCIA:	
NOMBRES Y APELLIDOS:	César Fortunato Mendoza Hernández

DATOS DEL CONTACTO:

Nombres y Apellidos	Carlos Sánchez	E-mail:	csanchez@reniec.gob.pe	Anexo	1488
Unidad Orgánica	GOR			RPM	#997204822
Ubicación:	Sede Ancash	Piso:	3	Dirección:	Jr. Ancash N° 354
Nombre del Evento	Lineamientos TUPA 2013			Expositor:	

TIPO DE SOLICITUD: PROGRAMACIÓN — Interna [X] Externa [ ] Nueva Instalación [ ] Reubicación [ ]

DATOS DEL REQUERIMENTO DE PROGRAMACIÓN

Fecha del Evento	09/01/2018	Hora Inicio	16:00:00	Hora Fin	17:00:00
	16/01/2018	Hora Inicio	16:00:00	Hora Fin	17:00:00
	23/01/2018	Hora Inicio	16:00:00	Hora Fin	17:00:00
	30/01/2018	Hora Inicio	16:00:00	Hora Fin	17:00:00
Tipo de Presentación	Video [ ]	PowerPoint / Excel [ ]			
	Otros			Desea grabar	[ ]

PROGRAMACIÓN INTERNA:

Datos de los Participantes Internos

1. Jefatura Regional Piura	[X] Contacto: Jimmy Martínez		Auditorio Institucional	[ ] Contacto:	
2. Jefatura Regional Trujillo	[ ] Contacto:		Facunto Regional	[ ] Contacto:	
3. Jefatura Regional Tarapoto	[X] Contacto:		CRIAS	[ ] Contacto:	
4. Jefatura Regional Iquitos	[ ] Contacto:		GOR	[X] Contacto: Carlos Sánchez	
5. Jefatura Regional Chimbote	[ ] Contacto:		GRC	[ ] Contacto:	
6. Jefatura Regional Huancayo	[X] Contacto: Pavel Torres		GRI	[ ] Contacto:	
7. Jefatura Regional Ayacucho	[ ] Contacto:		SGEN	[ ] Contacto:	
8. Jefatura Regional Arequipa	[ ] Contacto:		GRH	[ ] Contacto:	
9. Jefatura Regional Cusco	[ ] Contacto:		GAD	[ ] Contacto:	
11. Jefatura Regional Puno	[ ] Contacto:		GII	[ ] Contacto:	
12. Jefatura Regional Ica	[ ] Contacto:		GTH	[ ] Contacto:	
13. Jefatura Regional Huancavelica	[ ] Contacto:		GNI	[ ] Contacto:	
14. Jefatura Regional Pucallpa	[ ] Contacto:		OSDN	[ ] Contacto:	
15. Jefatura Regional Huánuco	[ ] Contacto:		EREP	[ ] Contacto:	
16. Jefatura Regional Arequipa	[ ] Contacto:		Sala Reuniones GII	[ ] Contacto:	
O. R. Chiclayo	[ ] Contacto:		Sala Capacitación GTH	[ ] Contacto:	
	[ ] Contacto:			[ ] Contacto:	

Nota: El servicio de Videoconferencia se deberá solicitar con 48 horas de anticipación. Se deberá registrar en el formato la fecha y hora, el o los contacto(s) de la(s) Unidad (es) Orgánica(s) con carácter obligatorio.

PROGRAMACIÓN EXTERNA:

Datos de los Participantes Externos

Entidad 1:	Ministerio de Relaciones Exteriores	Ubicación:	Av Universitaria N° 1452	Dirección IP:	200.15.100.20	Cisco Jabber	[ ]
Contacto:		E-mail:		Teléfono:		Zona Horaria (+/- GMT)	-05:00
Entidad 2:		Ubicación:		Dirección IP:		Cisco Jabber	[ ]
Contacto:		E-mail:		Teléfono:		Zona Horaria (+/- GMT)	
Entidad 3:		Ubicación:		Dirección IP:		Cisco Jabber	[ ]
Contacto:		E-mail:		Teléfono:		Zona Horaria (+/- GMT)	
Entidad 4:		Ubicación:		Dirección IP:		Cisco Jabber	[ ]
Contacto:		E-mail:		Teléfono:		Zona Horaria (+/- GMT)	
Entidad 5:		Ubicación:		Dirección IP:		Cisco Jabber	[ ]
Contacto:		E-mail:		Teléfono:		Zona Horaria (+/- GMT)	
Entidad 6:		Ubicación:		Dirección IP:		Cisco Jabber	[ ]
Contacto:		E-mail:		Teléfono:		Zona Horaria (+/- GMT)	

Ud. Puede verificar la zona horaria en: http://www.timeanddate.com/worldclock.

Nota: El servicio de Videoconferencia se deberá solicitar con 5 días hábiles de anticipación, debiendose registrar en el formato la fecha y hora, el o los contacto(s) Grupo Maximo de 6 participantes

SOPORTE DEL SERVICIO DE VIDEOCONFERENCIA:

Tipo de Solicitud:	Configuración [ ]		Reubicación Física [X]	Elaboración de Especificaciones Técnicas:	[ ]
	Unidad Orgánica Anterior	GOR			
	Unidad Orgánica Actual	GRI			
	Ubicación Física Anterior	Jr. Cusco			
	Ubicación Física Actual	Jr. Ancash			
Contacto Suplente		E-mail:	csanchez@reniec.gob.pe	Anexo 1608	

Justificación:

Nota: Para los casos de solicitud de Configuración, Reubicación Física y Nueva Instalación se deberá registrar la justificación.
La solicitud de requerimiento de Reubicación Física deberá ser solicitado con 5 días hábiles de anticipación.

SECRETARÍA GENERAL

GERENCIA PLANIFICACIÓN Y PRESUPUESTO

SUBGERENCIA DE OPERACIONES TELEMÁTICAS

SUBGERENCIA DE ASESORÍA ADMINISTRATIVA

GERENCIA ASESORÍA JURÍDICA

ANEXO Nº 05
FORMATO SERVICIO DE VPN

RENIEC
REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

FORMATO DEL SERVICIO VPN
(Alta, Renovación y Baja del servicio)

DATOS DEL FORMATO
CÓDIGO: GC-T-F-SVPN-04/SGOTA/GTI/RE Versión: 02 Fecha Emisión: 03/10/2013 Fecha Actualización: 01/02/2017

N° Formato: 00001/JRL/GOR FECHA DE SOLICITUD: 01/02/2017

DATOS DEL SOLICITANTE

GERENCIA/OFICINA: Gerencia de Operaciones Registrales

SUB GERENCIA/JEFATURA REGIONAL:

NOMBRES Y APELLIDOS: Raul Saco Vértiz

DATOS DEL CONTACTO:

Nombres y Apellidos: Jimmy Martinez Teléfono de contacto: 2105

DATOS DEL SERVIDOR CIVIL / LOCADOR DE SERVICIOS:

Nombres y Apellidos: Luis Escobar Teléfono de contacto:

Unidad Orgánica: GOR

Ubicación: Ayabaca Piso: Dirección: Franciso Bolognesi 181

DATOS DEL REQUERIMIENTO

Tipo de solicitud :

Periodo:

Alta [X] Del 01/10/2013 Al 30/11/2013 Baja [ ]

Renovación [ ] Del Al

Perfil de usuario

Funcionario [ ]

Administrador de Servicio Crítico [ ]

Nota: Los perfiles de funcionario y administrador de servicio crítico, tendrán acceso a los servicios VPN definidos en la Directiva "Servicios de Comunicación para Usuarios Finales".

Registrador [X] Acceso a: Horario Laboral: De 08:00:00 A 18:00:00

- [X] 1 Sistema Integrado de Tramite Documentario
- [X] 2 Módulo de Gestión de Agencias - SIO
- [ ] 3 Sistema Integrado de Registros Civiles
- [ ] 4 Otros (especificar) _____

Importante: El Gerente y/o Jefe de la Unidad Orgánica que autoriza y solicita la activación del servicio VPN para sus colaboradores, se hace responsable del buen uso del servicio por parte del colaborador.
El usuario final deberá tener en consideración y cumplir en estricto las políticas del servicio definidas en la Directiva "Servicios de Comunicación para Usuarios Finales".

***Nota:** Adjuntar al formato el "**Acta de confidencialidad del servicio VPN**" debidamente firmado por el usuario final.*
El servicio VPN se desactivará automáticamente una vez se cumpla el periodo establecido.

Justificación:

SECRETARÍA GENERAL

GERENCIA PLANIFICACIÓN Y PRESUPUESTO

SUBGERENTE DE OPERACIONES TELEMÁTICAS

SUB GERENCIA DE ASESORÍA ADMINISTRATIVA

GERENCIA ASESORÍA JURÍDICA

ANEXO N° 06

FORMATO ACTA DE CONFIDENCIALIDAD DEL SERVICIO VPN

ACTA DE CONFIDENCIALIDAD DEL SERVICIO VPN

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

- Mantener la confidencialidad de la información del RENIEC al que tengo acceso.
- No compartir mi usuario y clave de acceso al servicio VPN con otras personas.
- Cumplir con lo estipulado en la DI-327-GTI/021 "Servicio de Comunicación para Usuarios Finales".

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° 07
FORMATO DE SOLICITUD DE ANALISIS DE VULNERABILIDAD DE LOS SERVICIOS Y/O APLICACIONES WEB

SOLICITUD DE ANÁLISIS DE VULNERABILIDAD DE LOS SERVICIOS Y/O APLICACIONES WEB

RENIEC — REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

DATOS DEL FORMATO: CÓDIGO: MT-OT-[illegible]-[illegible] Versión: 01 Fecha de Emisión: [illegible] Fecha Actualización: 19/09/2017

N° SOLICITUD: 00001/GOR FECHA SOLICITUD: 19/09/2017 HORA SOLICITUD: 19/09/2017

DATOS DEL SOLICITANTE

GERENCIA:	Gerencia de Tecnología de la Información
SUB GERENCIA:	Ingeniería de Software
NOMBRES Y APELLIDOS:	Fanny Avila Rojas
LÍDER:	Soporte a la Implementación del Software
NOMBRES Y APELLIDOS:	Elizabeth Mendoza Allaga

DATOS DEL REQUERIMIENTO

NÚMERO DE REQUERIMIENTO INFORMÁTICO: N° 00001

Nuevo Desarrollo [ ] Mantenimiento [x]

SISTEMA/MÓDULO:

SISTEMA INTEGRADO OPERATIVO - ENTREGA DNI

URL: _____

PASE A PRE-PRODUCCIÓN/PRODUCCIÓN

Preproducción [x] Producción [ ]

OBSERVACIÓN:

_____

_____

_____

_____

_____

_____

SECRETARÍA GENERAL

GERENCIA PLANIFICACIÓN Y PRESUPUESTO

SUB GERENCIA DE ORGANIZACIONES Y MÉTODOS

SUB GERENCIA DE ASESORÍA ADMINISTRATIVA

GERENCIA ASESORÍA JURÍDICA

ANEXO N° 08
FORMATO DE REPORTE DE RESULTADOS DEL ANÁLISIS DE VULNERABILIDADES

Reporte de Resultado del Análisis de Vulnerabilidades

Reporte de Vulnerabilidad				N° 0301/2017/SGOT/GTI/RENIEC					
Tipo de Proyecto:	Desarrollo		Mantenimiento	X	Requerimiento:	N° 0913/2017/SGES/GTI/RENIEC			
Solicitud: N° 000		Fecha de Solicitud: 03/08/2017							
URL:									
Sistema:					Líder de Proyecto de Desarrollo de Software:	Jesus Obaya Coyunchan			
Fase CVS:	Construcción		Implantación						
	Pruebas de Seguridad	X	Pruebas de Seguridad						
Revisado por:	Igor Villarreal		Rol: Líder de Seguridad Informática		Fecha de Prueba:	03/08/2017			
Se comunica a:	Elizabeth Mendoza Aliaga		Rol: Líder de Proyecto de Soporte a la Implementación de Software		Fecha de Entrega:	03/08/2017			

	Resultado						Subsanación		
N°	Descripción de la Vulnerabilidad	Análisis de la Vulnerabilidad	Factor de Riesgo	Recomendación	Prioridad	Responsable	Fecha	Estado	Observaciones
1			Crítico		Alta			Atendido	
2									
3									
4									
5									
6									
7									
8									
9									
10									

ANEXO Nº 09
SOLICITUD DE PUBLICACIÓN A INTERNET DE LOS SERVICIOS Y/O APLICACIONES WEB

SOLICITUD DE PUBLICACIÓN A INTERNET DE LOS SERVICIOS Y/O APLICACIONES WEB

RENIEC

DATOS DEL FORMATO
CÓDIGO: RE-GT-I-SEG-04/TYS/GCT Versión 01 Fecha de Emisión 06/09/2017 Fecha Actualización 06/09/2017

Nº SOLICITUD: 00001/SGPRC/GRC FECHA SOLICITUD: 20/09/2017 HORA SOLICITUD: 20/09/2017

DATOS DEL SOLICITANTE

GERENCIA:	Gerencia de Tecnología de la Información
SUB GERENCIA:	Ingeniería de Software
NOMBRES Y APELLIDOS:	Fanny Avila Rojas
LÍDER:	Soporte a la Implementación del Software
NOMBRES Y APELLIDOS:	Elizabeth Mendoza Allaga

DATOS DEL REQUERIMIENTO

TIPO DE REQUERIMIENTO:

Alta del Servicio [X] Baja del servicio [ ]

NÚMERO DE REQUERIMIENTO INFORMÁTICO: Nº 00001

Nuevo Desarrollo [ ] Mantenimiento [X]

SISTEMA/MÓDULO:

SISTEMA DE REGISTROS CIVILES - NACIDO VIVO

URL:

PASE A PRE-PRODUCCIÓN/PRODUCCIÓN

Preproducción [ ] Producción [ ]

OBSERVACIÓN:

SECRETARÍA GENERAL

GERENCIA DE PLANIFICACIÓN Y PRESUPUESTO

SUBGERENTE DE OPERACIONES TELEMÁTICAS

SUB GERENCIA DE ASESORÍA ADMINISTRATIVA

GERENCIA ASESORÍA JURÍDICA

ANEXO Nº 10
FORMATO DE RATIFICACIÓN DE SERVICIOS DE COMUNICACIÓN PARA USUARIOS FINALES

RATIFICACIÓN DE SERVICIOS DE COMUNICACIÓN PARA USUARIOS FINALES - (AÑO)

RENIEC — REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

DATOS DEL FORMATO:
CÓDIGO: GC.T.F-RSC.06-SGCST/CTYRE Versión: 01 Fecha de Emisión: 22/09/2017 Fecha Actualización: 22/09/2017

Nº SOLICITUD: 00001/SGP/GTH FECHA SOLICITUD: 22/09/2017 HORA SOLICITUD: 22/09/2017

DATOS DEL SOLICITANTE

GERENCIA/OFICINA:

SUB GERENCIA/JEFATURA REGIONAL:

NOMBRES Y APELLIDOS:

ITEM	APELLIDOS Y NOMBRES	SERVICIOS					
		Perfil de Dominio	Correo Electrónico Nivel (1 ó 2)	Internet Nivel (1, 2,3 y 4)	Messenger	Telefonía IP Nivel (0, 1, 2 y 3)	VPN (1=SITD, 2=SIG, 3=RRCC y 4=Otros)

ANEXO Nº 11
CUADRO DE CONTROL DE CAMBIOS

DIRECTIVA "SERVICIOS DE COMUNICACIÓN PARA USUARIOS FINALES"	
IDENTIFICACIÓN DEL CAMBIO	
NUMERAL VIGENTE	**NUMERAL MODIFICADO**
I. OBJETIVO	**I. OBJETIVO**
II. ALCANCE	**II.ALCANCE**
III. BASE LEGAL	**III. BASE LEGAL**
Numeral 3.1	Numeral 3.1
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
Numeral 3.7	Numeral 3.6
No existía en esta versión	Numeral 3.7
No existía en esta versión	Numeral 3.9
Numeral 3.9	Numeral 3.10
Numeral 3.10	Numeral 3.11
Numeral 3.11	Numeral 3.12
Numeral 3.12	Eliminado.
Numeral 3.13	Numeral 3.13
No existía en esta versión	Numeral 3.14
Numeral 3.14	Numeral 3.15
Numeral 3.15	Numeral 3.16
Numeral 3.16	Numeral 3.17
Numeral 3.17	Numeral 3.18
No existía en esta versión	Numeral 3.19
Numeral 3.18	Numeral 3.20
IV. DEFINICIÓN DE TERMINOS	**IV. DEFINICIÓN DE TERMINOS**
No existía en esta versión	Numeral 4.2
Numeral 4.2	Numeral 4.3
Numeral 4.3	Numeral 4.4
Numeral 4.4	Numeral 4.5
Numeral 4.5	Numeral 4.6
Numeral 4.6	Eliminado
No existía en esta versión	Numeral 4.9
Numeral 4.9	Numeral 4.10
Numeral 4.10	Eliminado
No existía en esta versión	Numeral 4.14
Numeral 4.14	Eliminado
Numeral 4.15	Numeral 4.15
No existía en esta versión	Numeral 4.16
No existía en esta versión	Numeral 4.17
No existía en esta versión	Numeral 4.18
Numeral 4.16	Numeral 4.19
Numeral 4.17	Numeral 4.20

DIRECTIVA "SERVICIOS DE COMUNICACIÓN PARA USUARIOS FINALES"	
IDENTIFICACIÓN DEL CAMBIO	
NUMERAL VIGENTE	**NUMERAL MODIFICADO**
Numeral 4.18	Eliminado.
Numeral 4.19	Numeral 4.21
Numeral 4.20	Eliminado.
Numeral 4.21	Numeral 4.22
No existía en esta versión	Numeral 4.23
V. RESPONSABILIDADES	**V. RESPONSABILIDADES**
Numeral 5.2	Numeral 5.2
No existía en esta versión	Numeral 5.3
Numeral 5.3	Numeral 5.4
Numeral 5.4	Numeral 5.5
Numeral 5.5	Numeral 5.6
Numeral 5.6	Numeral 5.7
Numeral 5.7	Numeral 5.8
Numeral 5.8	Numeral 5.9
No existía en esta versión	Numeral 5.10
No existía en esta versión	Numeral 5.11
No existía en esta versión	Numeral 5.12
VI. DISPOSICIONES GENERALES	**VI. DISPOSICIONES GENERALES**
6.1 DEL SERVICIO DEL PERFIL DE DOMINIO	**6.1 DEL SERVICIO DEL PERFIL DE DOMINIO**
Numeral 6.1.1	Numeral 6.1.1
Numeral 6.1.2	Numeral 6.1.2
Numeral 6.1.3	Numeral 6.1.3
Numeral 6.1.4	Numeral 6.1.4
Numeral 6.1.5	Numeral 6.1.5
Numeral 6.1.6	Numeral 6.1.6
No existía en esta versión	Numeral 6.1.7
Numeral 6.1.7	Numeral 6.1.8
6.2 DEL SERVICIO DE CORREO ELECTRÓNICO	**6.2 DEL SERVICIO DE CORREO ELECTRÓNICO**
Numeral 6.2.1	Numeral 6.2.1
Numeral 6.2.2	Numeral 6.2.2
Numeral 6.2.3	Numeral 6.2.3
Numeral 6.2.4	Numeral 6.2.4
No existía en esta versión	Numeral 6.2.5
Numeral 6.2.5	Numeral 6.2.6
Numeral 6.2.6	Numeral 6.2.7
Numeral 6.2.7	Numeral 6.2.7
Numeral 6.2.8	Numeral 6.2.8
No existía en esta versión	Numeral 6.2.9
Numeral 6.2.9	Numeral 6.2.10
Numeral 6.2.10	Numeral 6.2.11
Numeral 6.2.11	Numeral 6.2.12
Numeral 6.2.12	Eliminado.
Numeral 6.2.13	Numeral 6.2.13
Numeral 6.2.14	Numeral 6.2.14

DIRECTIVA "SERVICIOS DE COMUNICACIÓN PARA USUARIOS FINALES"	
IDENTIFICACIÓN DEL CAMBIO	
NUMERAL VIGENTE	**NUMERAL MODIFICADO**
Numeral 6.2.15	Numeral 6.2.15
Numeral 6.2.16	Eliminado.
Numeral 6.2.17	Numeral 6.2.16
6.3 DEL SERVICIO DE MESSENGER INTERNO	**6.3 DEL SERVICIO DE MESSENGER INTERNO**
Numeral 6.3.1	Numeral 6.3.1
Numeral 6.3.1.2	Numeral 6.3.1.2
6.4 DEL SERVICIO DE ACCESO A INTERNET	**6.4 DEL SERVICIO DE ACCESO A INTERNET**
Numeral 6.4.1	Numeral 6.4.1
Numeral 6.4.2	Numeral 6.4.2
Numeral 6.4.3	Numeral 6.4.3
Numeral 6.4.4	Numeral 6.4.4
Numeral 6.4.5	Numeral 6.4.5
Numeral 6.4.6	Numeral 6.4.6
Numeral 6.4.7	Numeral 6.4.7
Numeral 6.4.8	Numeral 6.4.8
6.5 DEL SERVICIO DE TELEFONIA IP	**6.5 DEL SERVICIO DE TELEFONIA IP**
Numeral 6.5.1	Numeral 6.5.1
Numeral 6.5.2	Numeral 6.5.2
Numeral 6.5.3	Numeral 6.5.3
Numeral 6.5.4	Numeral 6.5.4
Numeral 6.5.5	Numeral 6.5.5
Numeral 6.5.6	Numeral 6.5.6
Numeral 6.5.7	Numeral 6.5.7
No existía en esta versión	Numeral 6.5.8
Numeral 6.5.9	Numeral 6.5.9
No existía en esta versión	Numeral 6.5.10
6.6 DEL SERVICIO DE INFRAESTRUCTURA DE COMUNICACIONES	**6.6 DEL SERVICIO DE INFRAESTRUCTURA DE COMUNICACIONES**
Numeral 6.6.1	Numeral 6.6.1
Numeral 6.6.2	Numeral 6.6.2
Numeral 6.6.3	Numeral 6.6.3
Numeral 6.6.4	Numeral 6.6.4
6.7 DEL SERVICIO DE VIDEO CONFERENCIA	**6.7 DEL SERVICIO DE VIDEO CONFERENCIA**
Numeral 6.7.2	Numeral 6.7.2
Numeral 6.7.3	Numeral 6.7.3
Numeral 6.7.4	Numeral 6.7.4
Numeral 6.7.5	Numeral 6.7.5
Numeral 6.7.7	Eliminado
6.8 DEL SERVICIO VPN (RED PRIVADA VIRTUAL)	**6.8 DEL SERVICIO VPN (RED PRIVADA VIRTUAL)**
Numeral 6.8.1	Numeral 6.8.1

DIRECTIVA "SERVICIOS DE COMUNICACIÓN PARA USUARIOS FINALES"	
IDENTIFICACIÓN DEL CAMBIO	
NUMERAL VIGENTE	**NUMERAL MODIFICADO**
Numeral 6.8.2	Numeral 6.8.2
Numeral 6.8.3	Numeral 6.8.3
Numeral 6.8.4	Numeral 6.8.4
No existía en esta versión	Numeral 6.8.6
Numeral 6.8.6	Numeral 6.8.7
Numeral 6.8.7	Numeral 6.8.8
6.9 DE LA ATENCIÓN PARA LA PUBLICACIÓN DE SERVICIOS Y/O APLICACIONES WEB	**6.9 DE LA ATENCIÓN PARA LA PUBLICACIÓN DE SERVICIOS Y/O APLICACIONES WEB**
No existía en esta versión	Numeral 6.9
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 ESPECÍFICAS	**VII. DISPOSICIONES ESPECÍFICAS**
7.1 DEL SERVICIO DEL PERFIL DE DOMINIO	**7.1 DEL SERVICIO DEL PERFIL DE DOMINIO**
Numeral 7.1.1	Numeral 7.1.1
No existía en esta versión	Numeral 7.1.2
Numeral 7.1.2	Numeral 7.1.3
Numeral 7.1.3	Numeral 7.1.4
Numeral 7.1.4	Numeral 7.1.5
Numeral 7.1.5	Numeral 7.1.6
No existía en esta versión	Numeral 7.1.7
Numeral 7.1.6	Numeral 7.1.8
Numeral 7.1.6	Numeral 7.1.9
Numeral 7.1.1	Numeral 7.1.10
Numeral 7.1.5	Numeral 7.1.11
No existía en esta versión	Numeral 7.1.12
7.2 DEL SERVICIO DE CORREO ELECTRÓNICO	**7.2 DEL SERVICIO DE CORREO ELECTRÓNICO**
Numeral 7.2.1	Numeral 7.2.1
Numeral 7.2.2	Numeral 7.2.2
Numeral 7.2.3	Numeral 7.2.3
Numeral 7.2.4	Numeral 7.2.4
Numeral 7.2.5	Eliminado.
Numeral 7.2.6	Numeral 7.2.5
Numeral 7.2.8	Numeral 7.2.6
Numeral 7.2.7	Numeral 7.2.7
Numeral 7.2.8	Numeral 7.2.8
No existía en esta versión	Numeral 7.2.9
Numeral 7.2.9	Numeral 7.2.10
No existía en esta versión	Numeral 7.2.11
7.3 DEL SERVICIO DE MESSENGER INTERNO	**7.3 DEL SERVICIO DE MESSENGER INTERNO**
Numeral 7.3.1	Numeral 7.3.1
Numeral 7.3.2	Numeral 7.3.2

DIRECTIVA "SERVICIOS DE COMUNICACIÓN PARA USUARIOS FINALES"	
IDENTIFICACIÓN DEL CAMBIO	
NUMERAL VIGENTE	**NUMERAL MODIFICADO**
Numeral 7.3.3	Numeral 7.3.3
No existía en esta versión	Numeral 7.3.4
7.4 DEL SERVICIO DE ACCESO A INTERNET	**7.4 DEL SERVICIO DE ACCESO A INTERNET**
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
Numeral 7.4.8	Eliminado
Numeral 7.4.9	Numeral 7.4.8
No existía en esta versión	Numeral 7.4.9
No existía en esta versión	Numeral 7.4.10
No existía en esta versión	Numeral 7.4.11
Numeral 7.4.8 y 7.4.10	Numeral 7.4.12
No existía en esta versión	Numeral 7.4.13
7.5 DEL SERVICIO DE TELEFONIA IP	**7.5 DEL SERVICIO DE TELEFONIA IP**
Numeral 7.5.1	Numeral 7.5.1
Numeral 7.5.2	Eliminado.
Numeral 7.5.3	Numeral 7.5.2
No existía en esta versión	Numeral 7.5.3
No existía en esta versión	Numeral 7.5.4
No existía en esta versión	Numeral 7.5.5
No existía en esta versión	Numeral 7.5.6
No existía en esta versión	Numeral 7.5.7
No existía en esta versión	Numeral 7.5.8
No existía en esta versión	Numeral 7.5.9
Numeral 7.5.4	Numeral 7.5.10
Numeral 7.5.5	Eliminado.
No existía en esta versión	Numeral 7.5.11
Numeral 7.5.6	Numeral 7.5.12
No existía en esta versión	Numeral 7.5.13
7.6 DEL SERVICIO DE INFRAESTRUCTURA DE COMUNICACIONES	**7.6 DEL SERVICIO DE INFRAESTRUCTURA DE COMUNICACIONES**
Numeral 7.6.1	Numeral 7.6.1
Numeral 7.6.3	Numeral 7.6.3
Numeral 7.6.4	Numeral 7.6.4
Numeral 7.6.5	Numeral 7.6.5
Numeral 7.6.6	Numeral 7.6.6
Numeral 7.6.6	Numeral 7.6.7
No existía en esta versión	Numeral 7.6.8
7.7 DEL SERVICIO DE VIDEO	**7.7 DEL SERVICIO DE VIDEO**

DIRECTIVA "SERVICIOS DE COMUNICACIÓN PARA USUARIOS FINALES"	
IDENTIFICACIÓN DEL CAMBIO	
NUMERAL VIGENTE	**NUMERAL MODIFICADO**
CONFERENCIA	**CONFERENCIA**
Numeral 7.7.1	Numeral 7.7.1
Numeral 7.7.2	Numeral 7.7.2
Numeral 7.7.5	Numeral 7.7.5
Numeral 7.7.6	Numeral 7.7.6
Numeral 7.7.7	Numeral 7.7.7
Numeral 7.7.8	Numeral 7.7.8
Numeral 7.7.9	Numeral 7.7.9
Numeral 7.7.10	Numeral 7.7.10
No existía en esta versión	Numeral 7.7.11
7.8 DEL SERVICIO VPN (RED PRIVADA VIRTUAL)	**7.8 DEL SERVICIO VPN (RED PRIVADA VIRTUAL)**
Numeral 7.8.1	Numeral 7.8.1
Numeral 7.8.2	Numeral 7.8.2
Numeral 7.8.3	Numeral 7.8.3
Numeral 7.8.4	Numeral 7.8.4
No existía en esta versión	Numeral 7.8.5
Numeral 7.8.5	Numeral 7.8.6
Numeral 7.8.6	Numeral 7.8.7
Numeral 7.8.7	Numeral 7.8.8
Numeral 7.8.8	Numeral 7.8.9
Numeral 7.8.9	Numeral 7.8.10
No existía en esta versión	Numeral 7.8.11
No existía en esta versión	Numeral 7.8.12
No existía en esta versión	Numeral 7.8.13
7.9 DE LA ATENCIÓN PARA LA PUBLICACIÓN DE SERVICIOS Y/O APLICACIONES WEB	**7.9 DE LA ATENCIÓN PARA LA PUBLICACIÓN DE SERVICIOS Y/O APLICACIONES WEB**
No existía en esta versión	Numeral 7.9.1
No existía en esta versión	Numeral 7.9.2
No existía en esta versión	Numeral 7.9.3
No existía en esta versión	Numeral 7.9.4
No existía en esta versión	Numeral 7.9.5
No existía en esta versión	Numeral 7.9.6
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
Anexo N° 04	Anexo N° 04
Anexo N° 05	Anexo N° 05
Anexo N° 06	Anexo N° 06
No existía en esta versión	Anexo N° 07

DIRECTIVA "SERVICIOS DE COMUNICACIÓN PARA USUARIOS FINALES"	
IDENTIFICACIÓN DEL CAMBIO	
NUMERAL VIGENTE	**NUMERAL MODIFICADO**
No existía en esta versión	Anexo N° 08
No existía en esta versión	Anexo N° 09
No existía en esta versión	Anexo N° 10
Anexo N° 07	Anexo N° 11