REGISTRO NACIONAL DE LAS PERSONAS -RENAP-
GUATEMALA, C.A.

ACUERDO DE DIRECCIÓN EJECUTIVA NÚMERO DE-785-2022
EL DIRECTOR EJECUTIVO DEL REGISTRO NACIONAL DE LAS PERSONAS -RENAP-

CONSIDERANDO:

Que de conformidad con la literal a) del artículo 134 de la Constitución Política de la República de Guatemala, las entidades autónomas actúan por delegación del Estado, y que tienen como una de las obligaciones el coordinar su política, con la política general del Estado y, en su caso, con la especial del Ramo a que correspondan; y de conformidad con lo regulado en los artículos 1 y 8 del Decreto número 90-2005 del Congreso de la República de Guatemala, Ley del Registro Nacional de las Personas, se crea el Registro Nacional de las Personas, como una entidad autónoma, de derecho público, con personalidad jurídica, patrimonio propio y plena capacidad para adquirir derechos y contraer obligaciones; son órganos del Registro: a) Directorio; b) Director Ejecutivo; c) Consejo Consultivo; d) Oficinas Ejecutoras; e) Direcciones Administrativas.

CONSIDERANDO:

Que de conformidad con los artículos 19, 20 literales a) y m) y 42 del Decreto número 90-2005 del Congreso de la República de Guatemala, Ley del Registro Nacional de las Personas, el Director Ejecutivo es el superior jerárquico administrativo, quien ejerce la representación legal y es el encargado de dirigir y velar por el funcionamiento normal e idóneo de la entidad; son funciones del Director Ejecutivo, cumplir y velar porque se cumplan los objetivos de la Institución, así como las leyes y reglamentos; y todas aquellas que sean necesarias para que la Institución alcance plenamente sus objetivos; siendo la Dirección de Informática y Estadística el ente encargado de dirigir las actividades relacionadas con el almacenamiento y procesamiento de los datos que se originen en el Registro Central de las Personas, en relación a su estado civil, capacidad civil y demás datos de identificación. Formula los planes y programas de la Institución en la materia de su competencia, informa sobre el cumplimiento de las metas institucionales programadas y elabora las estadísticas pertinentes.

CONSIDERANDO:

Que de conformidad con lo establecido en los artículos 50, y 82 del Acuerdo de Directorio número 80-2016 del Registro Nacional de las Personas, Reglamento de Organización y Funciones del Registro Nacional de las Personas, la Subdirección de Seguridad Informática, es la dependencia encargada de realizar actividades que permitan establecer controles de seguridad informática, por medio de la evaluación, análisis, diseño, implementación y monitoreo de los accesos a los sistemas de información, con el fin de garantizar la disponibilidad y confidencialidad de la información. Asimismo, el Director Ejecutivo aprobará los Manuales de Normas y Procedimientos y cualquier otro documento técnico administrativo de las dependencias del RENAP.

CONSIDERANDO:

Que la Dirección de Gestión y Control Interno del Registro Nacional de las Personas, solicitó la aprobación de la **"MANUAL DE NORMAS Y PROCEDIMIENTOS DEL DEPARTAMENTO DE SEGURIDAD INFORMÁTICA"**, Versión 03, de la Dirección de Informática y Estadística del Registro Nacional de las Personas, el cual tiene como objetivo proveer un documento técnico administrativo que sirva de apoyo y orientación para mantener la disponibilidad y confidencialidad de la información del RENAP, a través de controles de seguridad informática y la evaluación, análisis, diseño, implementación y monitoreo de los accesos a los sistemas de información.

POR TANTO:

Con base en lo considerado, normas legales citadas y lo que para el efecto establecen los artículos 134, 153 y 154 de la Constitución Política de la República de Guatemala; 1, 8, 19, 20 literales a) y m) y 42 del Decreto número 90-2005 del Congreso de la República de Guatemala, Ley del Registro Nacional de las Personas; 46, 47, 49, 50, 80, 82 y 84 del Acuerdo de Directorio Número 80-2016, Reglamento de Organización y Funciones del Registro Nacional de las Personas -RENAP-

ACUERDA:

Artículo 1. APROBAR bajo la estricta responsabilidad de la Dirección de Informática y Estadística, el contenido formulado por dicha Dirección dentro del documento denominado **"MANUAL DE NORMAS Y PROCEDIMIENTOS DEL DEPARTAMENTO DE SEGURIDAD INFORMÁTICA"**, Versión 03, de la Dirección de Informática y Estadística del Registro Nacional de las Personas.

Artículo 2. Se derogan todas las disposiciones anteriores que regulen la materia o que se opongan al presente Manual.

Artículo 3. Se instruye a las Direcciones involucradas, para que una vez se encuentre notificado el presente acuerdo, se realicen las diligencias necesarias a efecto de hacer posible la ejecución del mismo.

Artículo 4. Notifíquese a todas las Oficinas Ejecutoras, Direcciones Administrativas y Dependencias de Apoyo del Director Ejecutivo del RENAP, por medio de la Secretaría General de la Institución.

Artículo 5. El presente acuerdo entra en vigencia inmediatamente.

Dado en la ciudad de Guatemala, el cinco de diciembre de dos mil veintidós.

DOCTOR RODOLFO ESTUARDO ARRIAGA HERRERA
DIRECTOR EJECUTIVO

RENAP

SECRETARÍA GENERAL

CÉDULA DE NOTIFICACIÓN

En el municipio de Guatemala, departamento de Guatemala, el día ocho de diciembre de dos mil veintidós, siendo las once horas con cuatro minuto (s), constituido en: Calzada Roosevelt trece guión cuarenta y seis zona siete. Sede del **RENAP. Ciudad de Guatemala. NOTIFICO A** DIRECCION DE GESTIÓN Y CONTROL INTERNO. DEL REGISTRO NACIONAL DE LAS PERSONAS. El contenido del Acuerdo emitido por: Dirección Ejecutiva del Registro Nacional de las Personas número DE guión setecientos ochenta y cinco guión dos mil veintidós **(DE-785-2022),** de fecha cinco de diciembre de dos mil veintidós, por medio de cédula entregada a: Evelyn Morales, haciéndole entrega de las copias de ley que consta de UN folio (s), y quien de enterado (a) si firma.

LIC.LUIS ALFREDO MORALES.

Registro Nacional de las Personas
08 DIC 2022
DIRECCIÓN DE GESTIÓN Y CONTROL INTERNO
FIRMA: HORA: 11.04

RENAP
Registro Nacional de las Personas

DIRECCIÓN DE INFORMÁTICA Y ESTADÍSTICA

MANUAL DE NORMAS Y PROCEDIMIENTOS DEL DEPARTAMENTO DE SEGURIDAD INFORMÁTICA

Dr. Rodolfo Estuardo Arriaga Herrera
Director Ejecutivo
Registro Nacional de las Personas -RENAP-
Guatemala, Guatemala

Lic. Rudy Noé Mazariegos Lemus
Director de Gestión y Control Interno
Dirección de Gestión y Control Interno
Sede del RENAP, Guatemala, Guatemala

Ing. José Daniel Girón Miranda
Director de Informática y Estadística
Dirección de Informática y Estadística
Sede del RENAP, Guatemala, Guatemala

Lic. Juan Pablo Ulescas de la Cruz
Subdirector de Servicios Críticos
Dirección de Informática y Estadística
Sede del RENAP, Guatemala, Guatemala

Lic. Ricardo Bernabé Bercián Ramírez
Jefe de Organización y Métodos
Dirección de Gestión y Control Interno
Sede del RENAP, Guatemala, Guatemala

FECHA DE EMISIÓN:	Octubre 2022
CÓDIGO:	MNP-09-03-2022
VERSIÓN:	03

DEPARTAMENTO DE ORGANIZACIÓN Y MÉTODOS
DIRECCIÓN DE GESTIÓN Y CONTROL INTERNO

Contenido

1. Objetivo

Proveer un documento técnico administrativo que sirva de apoyo y orientación para mantener la disponibilidad y confidencialidad de la información del RENAP, a través de controles de seguridad informática y la evaluación, análisis, diseño, implementación y monitoreo de los accesos a los sistemas de información.

2. Campo de aplicación

El presente Manual es de observancia y aplicación obligatoria para los trabajadores del Departamento de Seguridad Informática de la Subdirección de Servicios Críticos de la Dirección de Informática y Estadística; asimismo, para quienes accedan a la red y servicios institucionales asociados[1].

3. Base legal

- Constitución Política de la República de Guatemala.
- Decreto número 89-2002 del Congreso de la República de Guatemala, Ley de Probidad y Responsabilidades de Funcionarios y Empleados Públicos.
- Decreto número 90-2005 del Congreso de la República de Guatemala, Ley del Registro Nacional de las Personas.
- Acuerdo de Directorio número 80-2016 del Registro Nacional de las Personas, Reglamento de Organización y Funciones del Registro Nacional de las Personas.
- Reglamento Interior de Trabajo del Registro Nacional de las Personas -RENAP- vigente, aprobado por medio de Acuerdo de Directorio del Registro Nacional de las Personas.

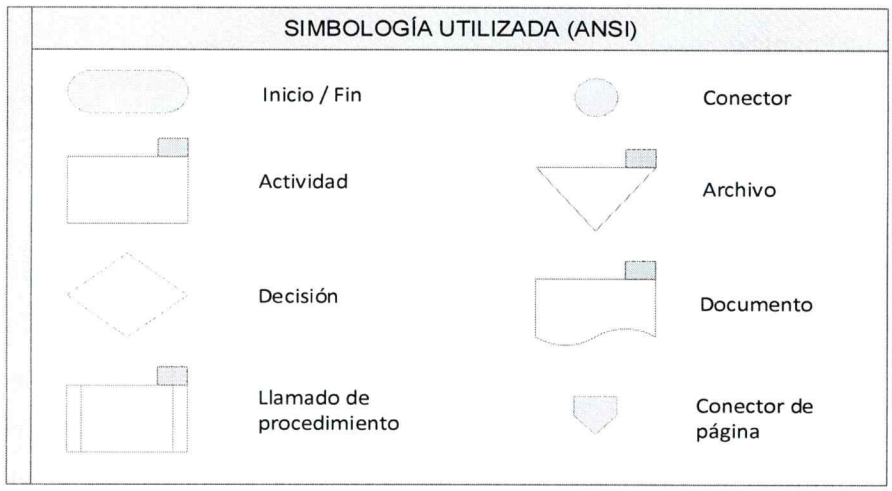
4. Monitoreo y seguimiento

Para garantizar la vigencia y efectividad de este Manual, el Jefe de Seguridad Informática, el Subdirector de Servicios Críticos y el Director de Informática y Estadística deberán solicitar la actualización oportuna para realizar la inclusión de ajustes y modificaciones que se consideren pertinentes.

[1] Servicios institucionales asociados: conjunto de sistemas que brindan apoyo a la prestación de servicios a través de red.

5. Simbología

Con el propósito de facilitar la representación visual de los procedimientos, se realizan los diagramas de flujo o flujogramas. La simbología utilizada para la construcción de los flujogramas del presente Manual es la siguiente:



6. Procedimiento para el acceso a la red y servicios institucionales asociados

6.1. Normas del procedimiento para el acceso a la red y servicios institucionales asociados

6.1.1. El acceso a la red y servicios institucionales asociados serán gestionados bajo el principio de cuentas únicas, personales e intransferibles.

6.1.2. El acceso a la red y servicios institucionales asociados deberán ser solicitados por medio de la "Boleta única todos los servicios" (ver anexo 1), la cual tendrá que ser completada en su totalidad y autorizada por el jefe inmediato y la máxima autoridad de la oficina ejecutora, dirección administrativa o dependencia de apoyo del Director Ejecutivo, cuando corresponda por el Director Ejecutivo.

6.1.3. Para el caso de solicitud de accesos para el personal contratado por servicios técnicos o profesionales (personal temporal 029) la máxima autoridad de la oficina ejecutora, dirección administrativa o dependencia de apoyo del Director Ejecutivo será quien autorice los accesos, siendo el contratista responsable del uso adecuado de los permisos que sean otorgados considerando los términos y condiciones de la "Boleta única todos los servicios".

6.1.4. Para solicitar VPN[2] por medio de la "Boleta única todos los servicios", ya sea fija o temporal, deberá describirse la justificación en el apartado de información adicional.

6.1.5. La solicitud de acceso al Sistema de Registro Civil -SIRECI- deberá contar con la autorización del Registrador Central de las Personas o el trabajador que este delegado para el efecto.

6.1.6. La solicitud de acceso al Sistema de Consulta de Documento Personal de Identificación -DPI- deberá contar con la autorización del Director de Procesos o el trabajador que este delegado para el efecto.

6.1.7. Los trabajadores del Departamento de Desarrollo de Sistemas deberán mantener un inventario actualizado de los sistemas de información y aplicaciones de software con los que opera la institución, así como, de los responsables de la administración de cada uno de estos.

[2] Virtual Private Network por sus siglas en inglés VPN (red privada virtual): es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando internet.

6.1.8. El Jefe de Seguridad Informática deberá designar al responsable de llevar el control interno de los usuarios nuevos y existentes, activos e inactivos.

6.1.9. Para que los trabajadores que cambien de puesto tengan permitida la ejecución de las funciones provistas en los sistemas conforme a su nuevo puesto, el Jefe de Seguridad Informática periódicamente coordinará que se efectúe la comparación de perfiles, generando los reportes correspondientes.

6.1.10. El Jefe de Seguridad Informática deberá remitir mensualmente a la Subdirección de Recursos Humanos, un listado de usuarios que fueron deshabilitados por inactividad para que se brinde el seguimiento respectivo.

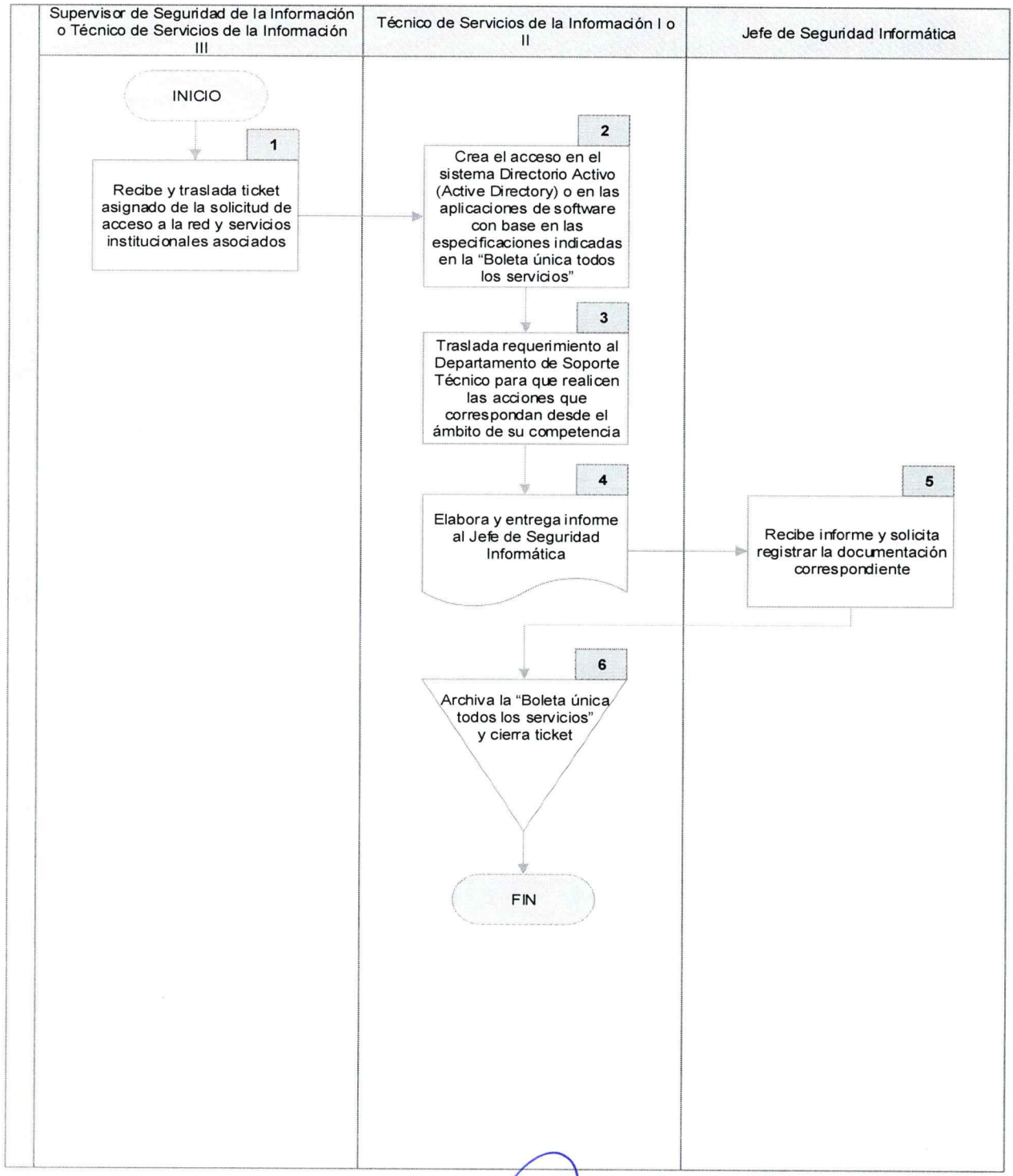
6.1.11. Los casos no previstos en el presente procedimiento serán resueltos en su orden por el Jefe de Seguridad Informática, el Subdirector de Servicios Críticos o por el Director de Informática y Estadística.

6.2. Descripción del procedimiento para el acceso a la red y servicios institucionales asociados

Responsable	Paso No.	Actividad
Supervisor de Seguridad de la Información o Técnico de Servicios de la Información III	1.	Recibe y traslada ticket[3] asignado de la solicitud de acceso a la red y servicios institucionales asociados.
Técnico de Servicios de la Información I o II	2.	Crea el acceso en el sistema Directorio Activo (Active Directory[4]) o en las aplicaciones de software con base en las especificaciones indicadas en la "Boleta única todos los servicios".
	3.	Traslada requerimiento al Departamento de Soporte Técnico para que realicen las acciones que correspondan desde el ámbito de su competencia.
	4.	Elabora y entrega informe al Jefe de Seguridad Informática.
Jefe de Seguridad Informática	5.	Recibe informe y solicita registrar la documentación correspondiente.
Técnico de Servicios de la Información I o II	6.	Archiva la "Boleta única todos los servicios" y cierra ticket.
		Fin del procedimiento.

[3] Ticket: número asignado a un trabajador para que se brinde un servicio de acuerdo con un sistema de turnos.
[4] Active Directory: herramienta informática para administrar de forma centralizada la red, permisos de acceso, dominios, impresoras compartidas, conexión a servidores, entre otros.

6.3. Flujograma del procedimiento para el acceso a la red y servicios institucionales asociados



7. Procedimiento para creación o cambio de autoridad de los Registradores Civiles de las Personas en el Sistema de Registro Civil -SIRECI-

7.1. Normas del procedimiento para creación o cambio de autoridad de los Registradores Civiles de las Personas en el Sistema de Registro Civil -SIRECI-

7.1.1. Los trabajadores del Departamento de Seguridad Informática serán los encargados de atender las solicitudes de cambio de autoridad de los Registradores Civiles de las Personas.

7.1.2. Para el cambio de autoridad, el Registro Central de las Personas deberá presentar a la Dirección de Informática y Estadística la documentación siguiente:

a) Nombramiento con el número de Acuerdo de Dirección Ejecutiva respectivo o acta administrativa suscrita por el Subdirector de Recursos Humanos y Registrador Central de las Personas, este último caso, cuando sea por ampliación de competencia.
b) "Boleta única todos los servicios" (ver anexo 1).
c) "Boleta de autorización para enrolamiento sin huella dactilar o amputación" (ver anexo 2).
d) Fotocopia del Documento Personal de Identificación -DPI- del trabajador indicado en el acuerdo o acta administrativa.
e) Firma para creación o cambio de autoridad de Registrador Civil de las Personas en el Sistema de Registro Civil -SIRECI- (ver anexo 3).

7.1.3. En los casos de retorno de autoridad, si el nombramiento o el acta de ampliación de competencia no tiene definida la temporalidad del cambio de autoridad, el Registro Central de las Personas deberá presentar a la Dirección de Informática y Estadística el nombramiento con el número de Acuerdo de Dirección Ejecutiva respectivo o acta administrativa suscrita por el Subdirector de Recursos Humanos y Registrador Central de las Personas.

7.1.4. Los trabajadores del Departamento de Seguridad Informática deberán realizar el cambio de autoridad en el Sistema de Registro Civil -SIRECI- cuando el Registrador Civil de las Personas inicie la función registral.

7.1.5. Se podrán solicitar con carácter urgente, cambios de autoridad en el Sistema de Registro Civil -SIRECI- al Jefe de Seguridad Informática a través de correo electrónico institucional en los casos siguientes:

a) Por suspensión de labores.
b) Por rescisión de contrato, renuncia o abandono de labores.
c) Fallecimiento del Registrador Civil de las Personas.

d) Fallecimiento de un familiar del Registrador Civil de las Personas, conforme a los casos establecidos en el Reglamento Interior de Trabajo del Registro Nacional de las Personas -RENAP- vigente.

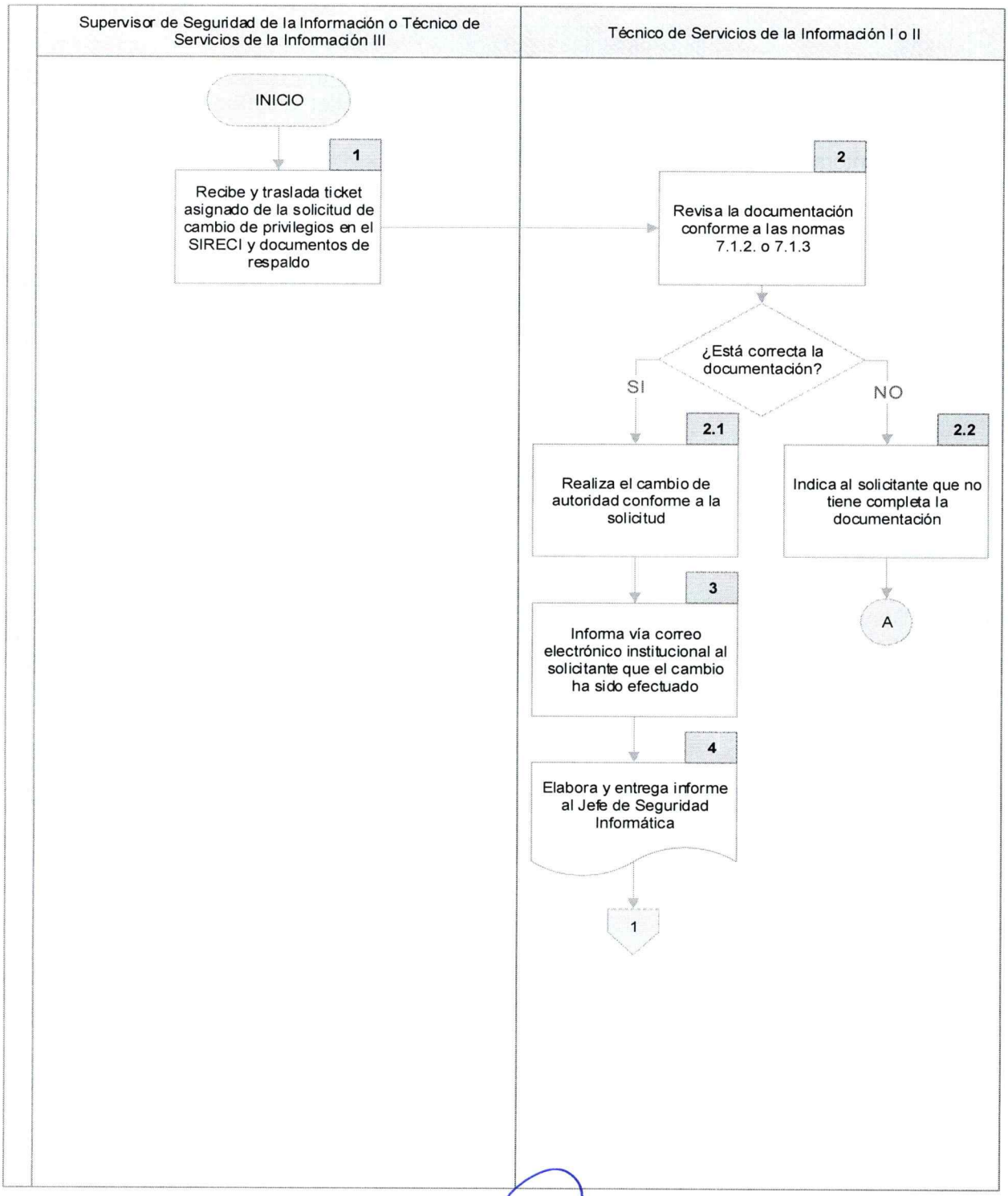
Serán revertidos los cambios efectuados, si la documentación descrita en la norma 7.1.2. no se traslada el día hábil siguiente.

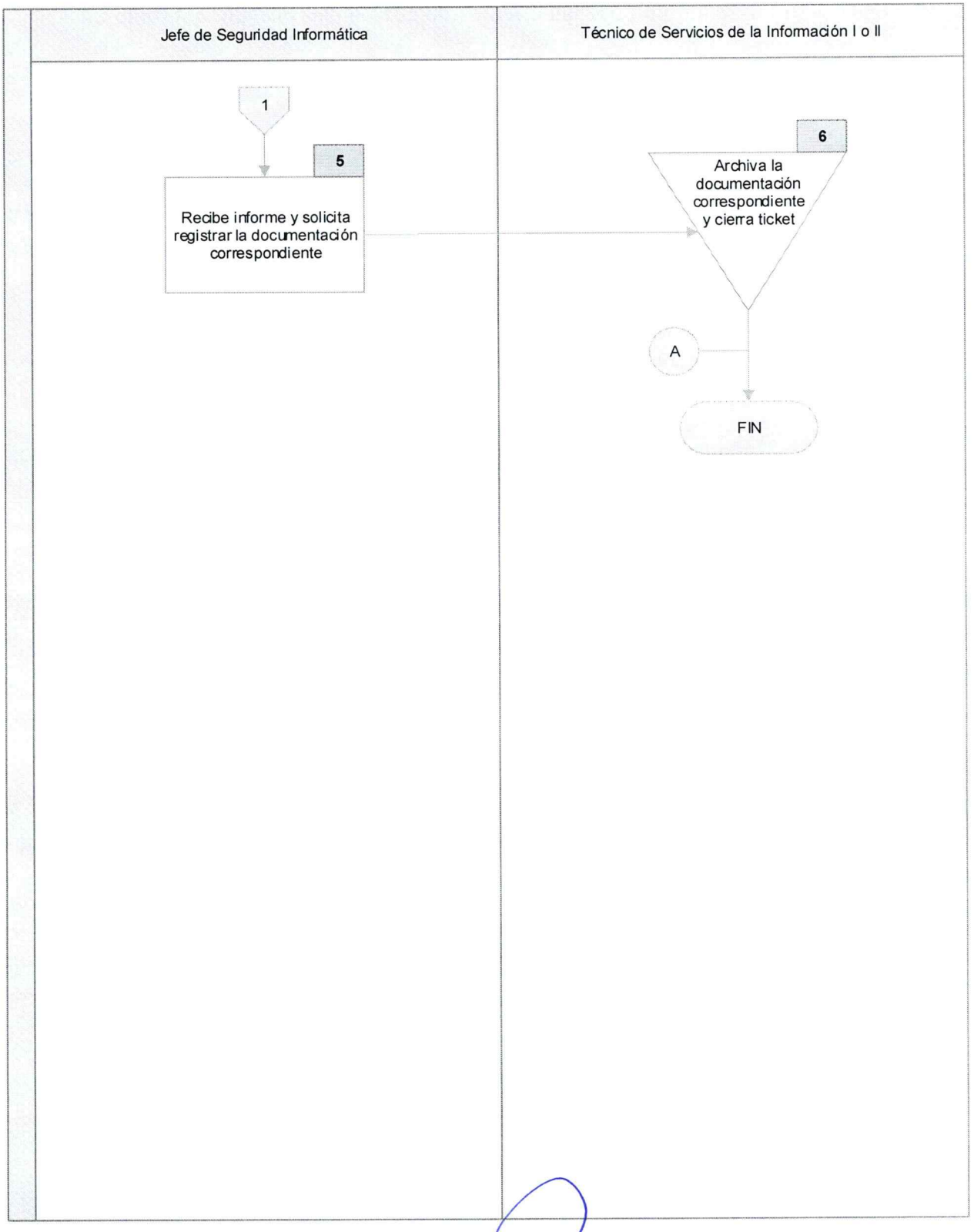
7.1.6. Los casos no previstos en el presente procedimiento serán resueltos en su orden por el Jefe de Seguridad Informática, el Subdirector de Servicios Críticos o por el Director de Informática y Estadística.

7.2. Descripción del procedimiento para creación o cambio de autoridad de los Registradores Civiles de las Personas en el Sistema de Registro Civil -SIRECI-

Responsable	Paso No.	Actividad
Supervisor de Seguridad de la Información o Técnico de Servicios de la Información III	1.	Recibe y traslada ticket asignado de la solicitud de cambio de privilegios en el SIRECI y documentos de respaldo.
Técnico de Servicios de la Información I o II	2.	Revisa la documentación conforme a las normas 7.1.2. o 7.1.3.
	2.1	Si está correcta la documentación, realiza el cambio de autoridad conforme a la solicitud. Continúa en el paso No. 3.
	2.2	No está correcta la documentación, indica al solicitante que no tiene completa la documentación. Fin del procedimiento.
	3.	Informa vía correo electrónico institucional al solicitante que el cambio ha sido efectuado.
	4.	Elabora y entrega informe al Jefe de Seguridad Informática.
Jefe de Seguridad Informática	5.	Recibe informe y solicita registrar la documentación correspondiente.
Técnico de Servicios de la Información I o II	6.	Archiva la documentación correspondiente y cierra ticket.
		Fin del procedimiento.

7.3. Flujograma del procedimiento para creación o cambio de autoridad de los Registradores Civiles de las Personas en el Sistema de Registro Civil -SIRECI-





Elaborado por:	Revisado por:	Revisado por:	Validado por:	Validado por:	Aprobado por:
Departamento de Organización y Métodos	Jefe de Organización y Métodos	Director de Gestión y Control Interno	Subdirector de Servicios Críticos	Director de Informática y Estadística	Director Ejecutivo

8. Procedimiento para administrar las cuentas de correo electrónico institucional

8.1. Normas del procedimiento para administrar las cuentas de correo electrónico institucional

8.1.1. El correo electrónico institucional deberá ser solicitado por medio de la "Boleta única todos los servicios" (ver anexo 1), la cual tendrá que estar completada en su totalidad y autorizada por el jefe inmediato y la máxima autoridad de la oficina ejecutora, dirección administrativa o dependencia de apoyo del Director Ejecutivo, cuando corresponda por el Director Ejecutivo.

8.1.2. Posterior a la recepción de la "Boleta única todos los servicios", el correo electrónico institucional será creado en un plazo no mayor a cuarenta y ocho (48) horas.

8.1.3. El Departamento de Seguridad Informática validará que los nombres asignados para los correos electrónicos institucionales sean únicos.

8.1.4. Para que un trabajador pueda tener más de una cuenta de correo electrónico institucional, la máxima autoridad de la oficina ejecutora, dirección administrativa o dependencia de apoyo del Director Ejecutivo deberá solicitarlo por medio de oficio a la Dirección Informática y Estadística.

8.1.5. El Departamento de Seguridad Informática será responsable de administrar el servicio del correo electrónico institucional (transporte-origen-destino, servicio de entrega de mensajes).

8.1.6. Los sistemas de correo electrónico institucional serán protegidos por un sistema de seguridad informático autorizado por el Director de Informática y Estadística.

8.1.7. El acceso al correo electrónico institucional será proporcionado con el fin de realizar actividades estrictamente laborales.

8.1.8. Cada usuario es responsable de mantener la privacidad de su cuenta de correo electrónico, así como, resguardar y hacer el uso adecuado de la información, evitando propiciar la fuga de información que pueda comprometer y poner en riesgo a la institución.

8.1.9. La información recibida, transmitida y almacenada en los servidores del correo electrónico institucional estará sujeta a auditorías.

8.1.10. El Departamento de Soporte Técnico realizará la configuración del equipo de cómputo de cada trabajador como .pst1[5], a excepción de las cuentas de directores, subdirectores y jefes, a quienes se les configurará como .ost2[6].

8.1.11. El Departamento de Seguridad Informática podrá realizar modificaciones a la plataforma del correo electrónico institucional por actualización de versión, por fallas, entre otros.

8.1.12. De acuerdo con la configuración del correo electrónico que efectúe el Departamento de Seguridad Informática, todo mensaje de manera predeterminada tendrá al pie de página el texto siguiente:

"Este correo electrónico, su contenido y anexos son CONFIDENCIALES y pueden contener información PRIVILEGIADA para uso exclusivo de su destinatario. Si ha recibido este correo por error o si existe error en el destinatario, por favor no lo copie o distribuya, ni realice ninguna acción relacionada con el mismo. En su lugar, por favor notifíquelo al remitente y bórrelo de su sistema en forma inmediata. Las opiniones expresadas en este correo son responsabilidad exclusiva de su autor y no son necesariamente compartidas o apoyadas por el Registro Nacional de las Personas -RENAP-, quien no asume a través de este correo obligaciones ni se responsabiliza del contenido del mismo. El RENAP se reserva las acciones legales que correspondan contra todo tercero que acceda de forma ilegítima al contenido de cualquier mensaje externo procedente de la misma. Para información y consultas visite nuestro sitio web www.renap.gob.gt".

8.1.13. No se deberá utilizar el correo electrónico de la institución para enviar información de tipo confidencial.

8.1.14. La clasificación de los niveles de capacidad para el envío de correos electrónicos, según el puesto que se ocupa, es la siguiente:

NIVEL	SEGMENTO	CAPACIDAD DE ENVÍO
Básico	Trabajador del área operativa	3 MB
Preferente	Trabajador del área operativa*	5 MB
Jefes	Jefe de departamento	7 MB

[5].pst1: tipo de configuración del correo electrónico que almacena los mensajes y otros elementos en el equipo.
[6].ost2: tipo de configuración del correo electrónico que almacena los elementos en un servidor o medio móvil.

NIVEL	SEGMENTO	CAPACIDAD DE ENVÍO
Directores	Directores, Registrador Central de las Personas, Auditor Interno, Inspector General, Secretario General y Comunicador Social	20 MB
VIP	Director Ejecutivo, miembros del Directorio y asesores de Dirección Ejecutiva	25 MB

* Preferente: cuando el usuario requiera una capacidad diferente a las definidas para el envío de adjuntos en el correo electrónico institucional, deberá solicitarlo mediante la "Boleta única todos los servicios" para la modificación.

Cuando se requiera una capacidad distinta a los niveles establecidos, se deberá solicitar mediante la "Boleta única todos los servicios" acompañada de un oficio explicando detalladamente sobre el uso que se le dará y las razones del porqué de la solicitud, con las firmas respectivas del jefe inmediato y la máxima autoridad de la oficina ejecutora, dirección administrativa o dependencia de apoyo del Director Ejecutivo.

8.1.15. Para que un trabajador pueda enviar un correo electrónico a más de diez (10) destinatarios (exceptuando los directores que tendrán un máximo de 20 destinatarios), la máxima autoridad de la oficina ejecutora, dirección administrativa o dependencia de apoyo del Director Ejecutivo deberá solicitarlo por medio de oficio a la Dirección de Informática y Estadística.

8.1.16. El Jefe de Seguridad Informática será el encargado de designar al trabajador que deberá realizar la depuración de las cuentas en el sistema del correo electrónico institucional, así como, la inhabilitación de los usuarios que hayan sido dados de baja en la institución.

8.1.17. Los mensajes del correo electrónico institucional no deberán ser eliminados, considerando que, la información que se encuentra en el equipo del usuario es propiedad de la institución.

8.1.18. Todo usuario con acceso a correo electrónico institucional deberá abstenerse de enviar, reenviar, responder archivos adjuntos con extensiones (.exe, .bat, .sys, .vsb, .com o cualquier otro ejecutable) o que sean de dudosa procedencia, sin autorización de la Dirección de Informática y Estadística.

8.1.19. El usuario no deberá colocar anuncios en su cuenta de correo electrónico institucional, que resten profesionalismo o que dañen la imagen institucional.

8.1.20. El Comunicador Social designará a los trabajadores a su cargo para el envío de correos masivos, de lo cual se deberá informar a la Dirección de Informática y Estadística mediante oficio.

8.1.21. Cualquier usuario ajeno a Comunicación Social que derivado de sus funciones requiera enviar correos masivos, deberá solicitar la autorización mediante oficio a la Dirección de Informática y Estadística.

8.1.22. Para la gestión de buzón de correo electrónico adicional o lista de distribución con propósitos especiales, se deberá solicitar por medio de oficio dirigido a la Dirección de Informática y Estadística.

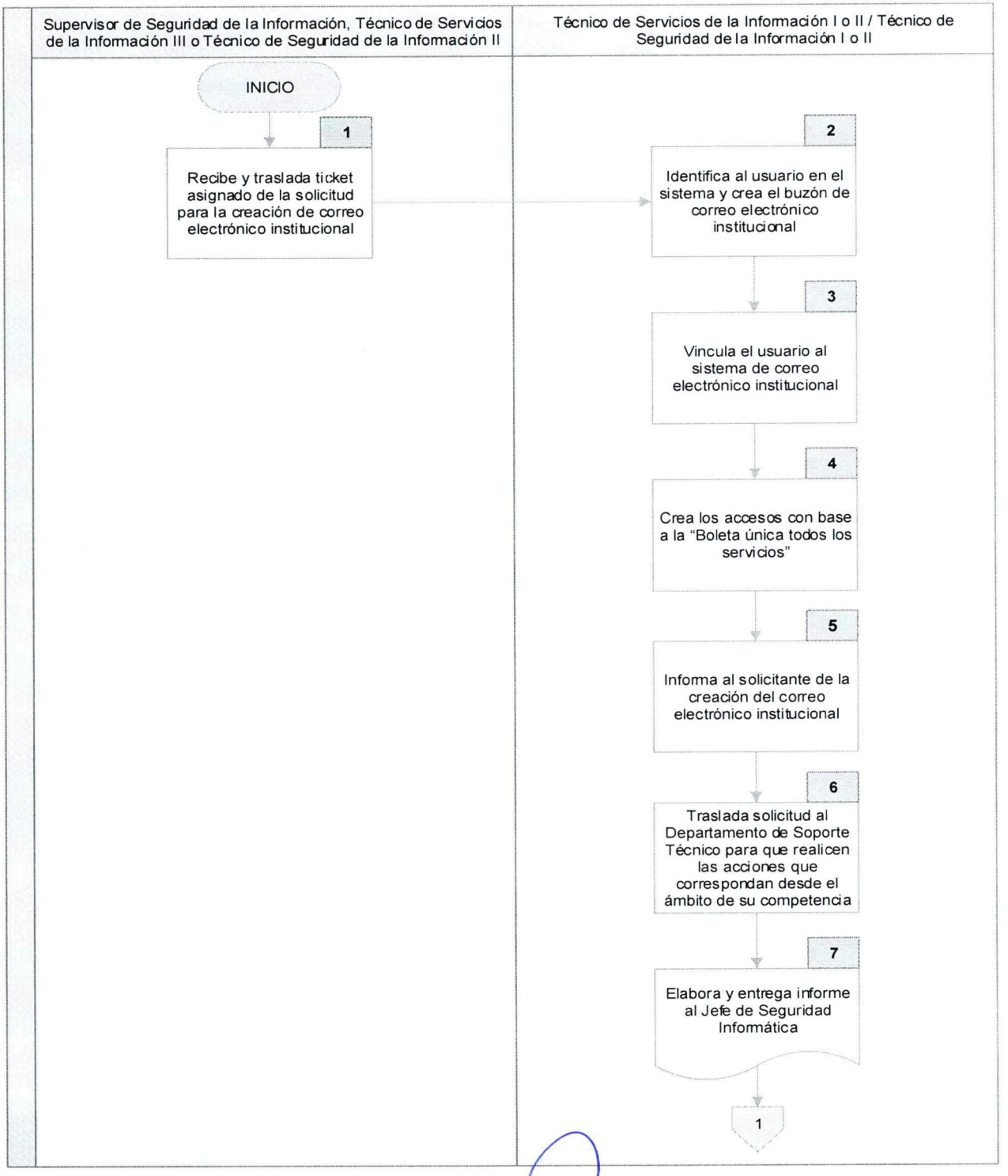
8.1.23. Los trabajadores a los que se le asigne un correo electrónico institucional estarán sujetos al cumplimiento de los términos e indicaciones descritos en la "Boleta única todos los servicios".

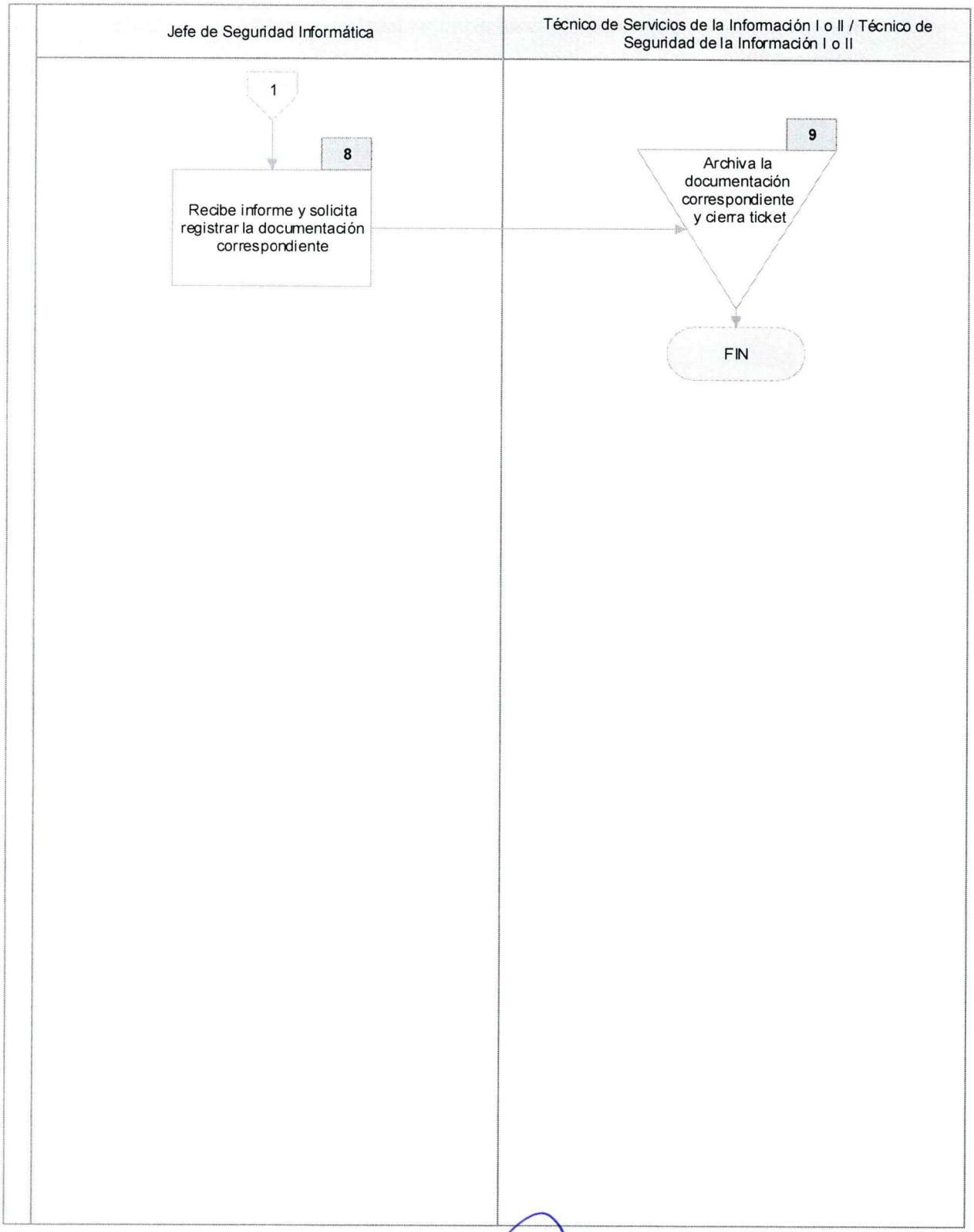
8.1.24. Los casos no previstos en el presente procedimiento serán resueltos en su orden por el Jefe de Seguridad Informática, el Subdirector de Servicios Críticos o por el Director de Informática y Estadística.

8.2. Descripción del procedimiento para administrar las cuentas de correo electrónico institucional

Responsable	Paso No.	Actividad
Supervisor de Seguridad de la Información, Técnico de Servicios de la Información III o Técnico de Seguridad de la Información II	1.	Recibe y traslada ticket asignado de la solicitud para la creación de correo electrónico institucional.
Técnico de Servicios de la Información I o II / Técnico de Seguridad de la Información I o II	2.	Identifica al usuario en el sistema y crea el buzón de correo electrónico institucional.
	3.	Vincula el usuario al sistema de correo electrónico institucional.
	4.	Crea los accesos con base a la "Boleta única todos los servicios".
	5.	Informa al solicitante de la creación del correo electrónico institucional.
	6.	Traslada solicitud al Departamento de Soporte Técnico para que realicen las acciones que correspondan desde el ámbito de su competencia.
	7.	Elabora y entrega informe al Jefe de Seguridad Informática.
Jefe de Seguridad Informática	8.	Recibe informe y solicita registrar la documentación correspondiente.
Técnico de Servicios de la Información I o II / Técnico de Seguridad de la Información I o II	9.	Archiva la documentación correspondiente y cierra ticket.
		Fin del procedimiento.

8.3. Flujograma del procedimiento para administrar las cuentas de correo electrónico institucional




Jefe de Seguridad Informática
Técnico de Servicios de la Información I o II / Técnico de Seguridad de la Información I o II
1
8
Recibe informe y solicita registrar la documentación correspondiente
9
Archiva la documentación correspondiente y cierra ticket
FIN

9. Procedimiento para la baja definitiva de un usuario en los sistemas de red

9.1. Normas del procedimiento para la baja definitiva de un usuario en los sistemas de red

9.1.1. El Departamento de Seguridad Informática será el encargado de administrar la información que se encuentra en el Directorio Activo (Active Directory).

9.1.2. El Departamento de Seguridad Informática será el responsable de la depuración periódica de cuentas inactivas.

9.1.3. La Dirección de Informática y Estadística será responsable de proporcionarle al Departamento de Gestión de Recursos Humanos una aplicación para la inactivación de usuarios, la cual será utilizada cuando se dé por terminada la relación laboral de los trabajadores o la finalización de contratos. De existir inconvenientes con la aplicación, el Departamento de Gestión de Recursos Humanos solicitará por medio de correo electrónico institucional al Departamento de Seguridad Informática que se efectúe la inactivación.

9.1.4. Además de lo establecido en la norma 9.1.3, el Departamento de Gestión de Recursos Humanos deberá trasladar a la Dirección de Informática y Estadística la "Boleta de baja definitiva del usuario de los sistemas" (ver anexo 4), para que se realicen las acciones pertinentes, logrando así un mejor control de los usuarios y accesos.

9.1.5. El Departamento de Seguridad Informática verificará que la baja definitiva se haya efectuado, con base a los documentos remitidos por el Departamento de Gestión de Recursos Humanos.

9.1.6. El Departamento de Seguridad Informática deberá deshabilitar y trasladar el buzón de correo electrónico institucional a otra unidad organizativa (objeto de directorio activo, dentro del mismo dominio) cuando las personas hayan finalizado la relación laboral con el RENAP o dejado de prestar sus servicios.

9.1.7. En los casos de cambio de puesto (fijo o temporal), el Departamento de Gestión de Recursos Humanos informará al trabajador sobre la baja de su usuario al finalizar la jornada laboral y entregará la "Boleta de baja definitiva del usuario de los sistemas" a la Dirección de Informática y Estadística.

9.1.8. El trabajador deberá presentar la "Boleta de baja definitiva del usuario de los sistemas" y la "Boleta única todos los servicios" a la Dirección de Informática y Estadística, en la que indique el nuevo puesto y accesos a los sistemas requeridos.

9.1.9. El Departamento de Seguridad Informática registrará la fecha en que fueron dados de baja los usuarios a los sistemas de red.

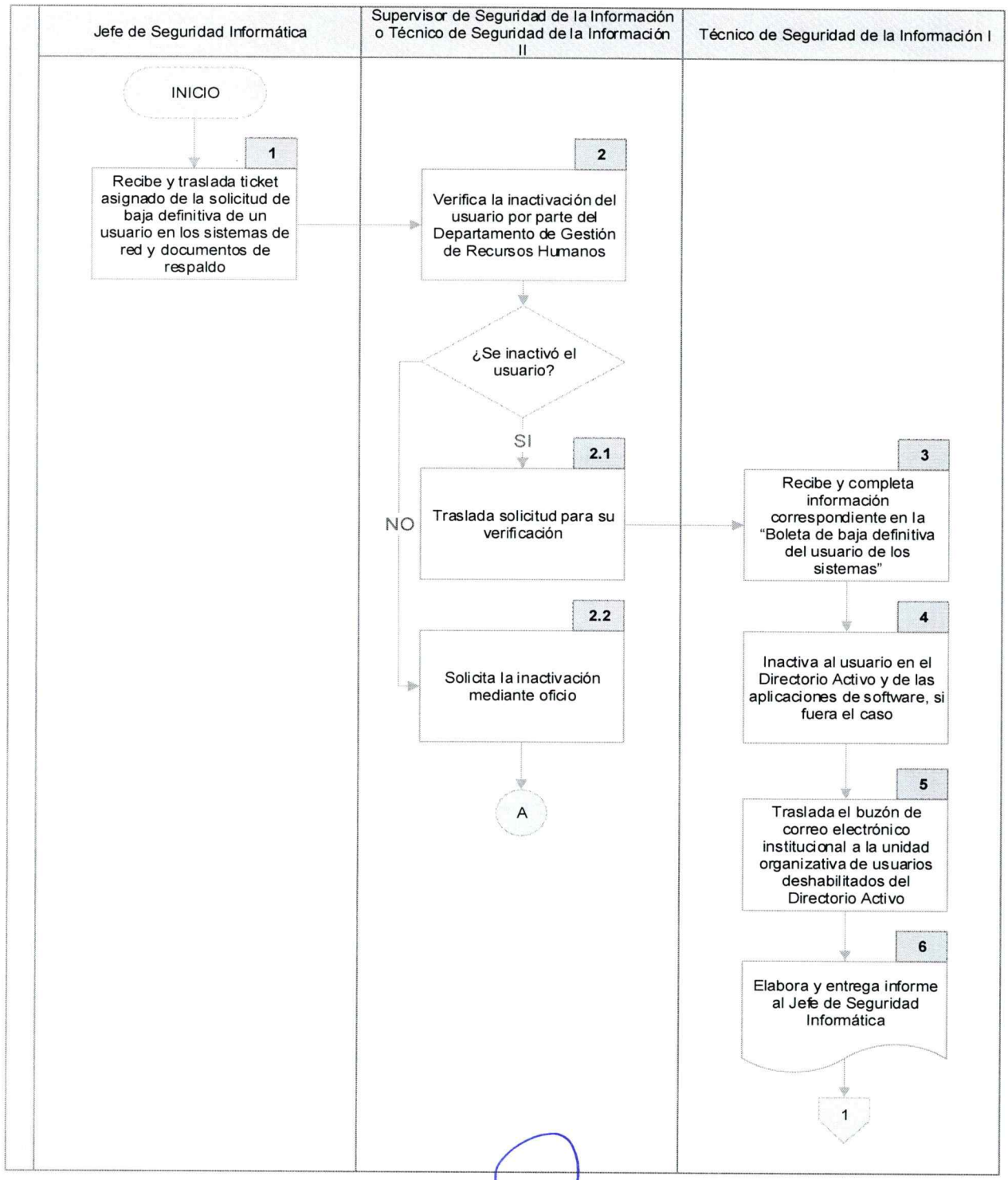
9.1.10. Por recomendación de Inspectoría General, de la máxima autoridad de las oficinas ejecutoras, direcciones administrativas y de las dependencias de apoyo del Director Ejecutivo en donde labora la persona o del Departamento de Seguridad Informática, se podrá inactivar a usuarios que pongan en peligro la confidencialidad, integridad o disponibilidad de la seguridad de la información.

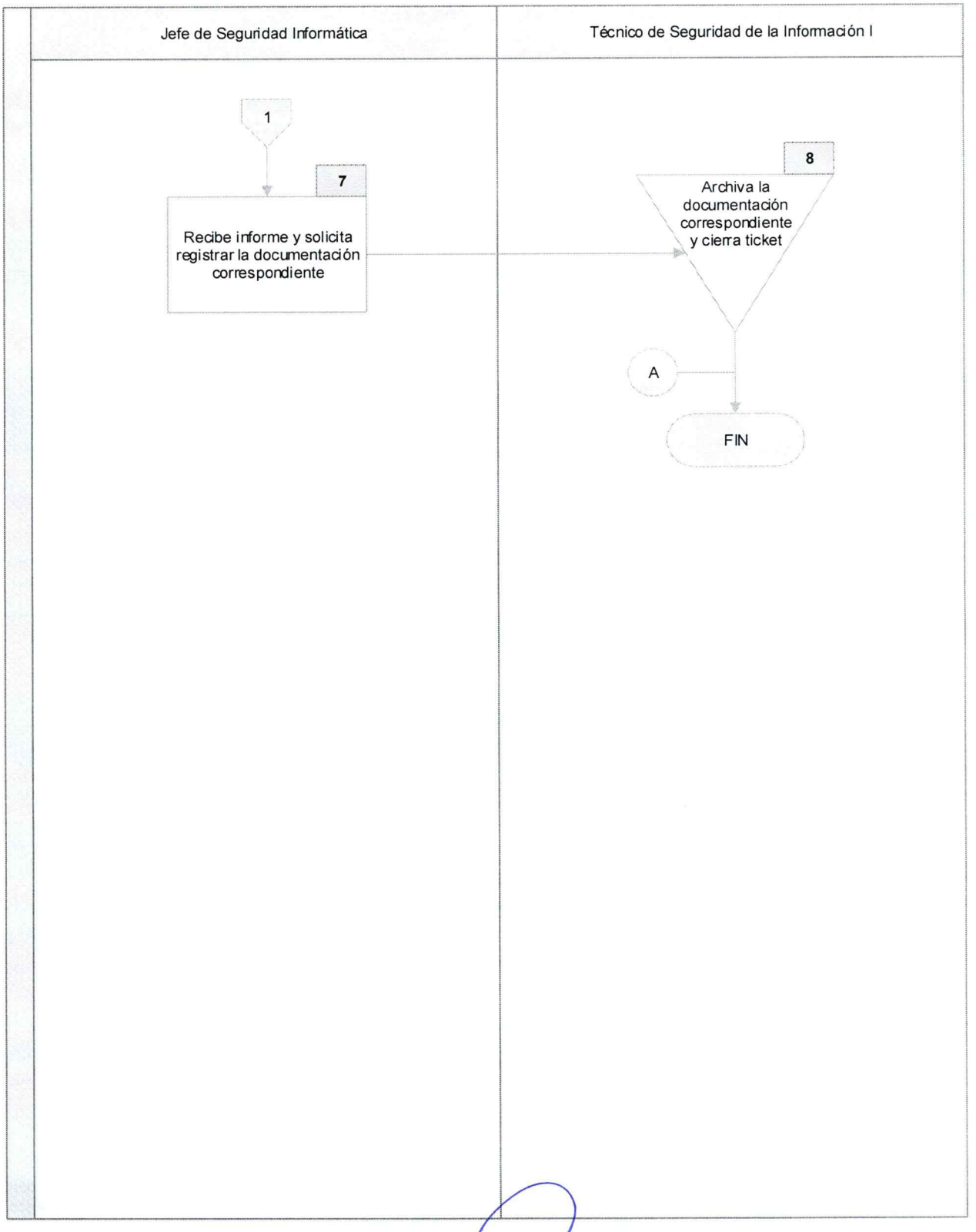
9.1.11. Los casos no previstos en el presente procedimiento serán resueltos en su orden por el Jefe de Seguridad Informática, el Subdirector de Servicios Críticos o por el Director de Informática y Estadística.

9.2. Descripción del procedimiento para la baja definitiva de un usuario en los sistemas de red

Responsable	Paso No.	Actividad
Jefe de Seguridad Informática	1.	Recibe y traslada ticket asignado de la solicitud de baja definitiva de un usuario en los sistemas de red y documentos de respaldo.
Supervisor de Seguridad de la Información o Técnico de Seguridad de la Información II	2.	Verifica la inactivación del usuario por parte del Departamento de Gestión de Recursos Humanos.
	2.1	Si se inactivó el usuario, traslada solicitud para su verificación. Continúa en el paso No. 3.
	2.2	No se inactivó el usuario, solicita la inactivación mediante oficio. Fin del procedimiento.
Técnico de Seguridad de la Información I	3.	Recibe y completa información correspondiente en la "Boleta de baja definitiva del usuario de los sistemas".
	4.	Inactiva al usuario en el Directorio Activo y de las aplicaciones de software, si fuera el caso.
	5.	Traslada el buzón de correo electrónico institucional a la unidad organizativa de usuarios deshabilitados del Directorio Activo.
	6.	Elabora y entrega informe al Jefe de Seguridad Informática.
Jefe de Seguridad Informática	7.	Recibe informe y solicita registrar la documentación correspondiente.
Técnico de Seguridad de la Información I	8.	Archiva la documentación correspondiente y cierra ticket.
		Fin del procedimiento.

9.3. Flujograma del procedimiento para la baja definitiva de un usuario en los sistemas de red





Elaborado por:	Revisado por:	Revisado por:	Validado por:	Validado por:	Aprobado por:
Departamento de Organización y Métodos	Jefe de Organización y Métodos	Director de Gestión y Control Interno	Subdirector de Servicios Críticos	Director de Informática y Estadística	Director Ejecutivo

10. Procedimiento para la autorización de medios extraíbles

10.1. Normas del procedimiento para la autorización de medios extraíbles

10.1.1. Las solicitudes de uso de medios extraíbles[7] deberán efectuarse mediante el formulario de "Autorización de medios extraíbles" (ver anexo 5).

10.1.2. El Departamento de Seguridad Informática es el responsable del control y monitoreo de los medios extraíbles autorizados. Asimismo, para que el medio extraíble sea utilizado deberá ser escaneado con el software específico para el control de virus o malware[8] instalado en el equipo.

10.1.3. El trabajador autorizado para el uso de medios extraíbles será responsable de la confidencialidad e integridad de la información.

10.1.4. La autorización para el uso de medios extraíbles tendrá los niveles siguientes:

SEGMENTO	NIVELES DE USO
Usuario	Poseen permiso para ingresar con su usuario a los distintos equipos que tenga asignados y utilizar todo tipo de dispositivo que tenga asignado.
Equipo	El usuario puede ingresar en distintos equipos y tiene permiso únicamente para el dispositivo autorizado.
Dispositivo	El dispositivo es reconocido por la red institucional.

Nota: El medio extraíble de uso personal de los trabajadores de la institución no podrá ser instalado o utilizado en las estaciones de trabajo, esto incluye memorias USB, dispositivos de almacenamiento externo, reproductores multimedia, entre otros.

10.1.5. Los puertos tipo USB serán bloqueados para la transmisión de datos con excepción de los dispositivos autenticados y autorizados.

10.1.6. La autorización de medios extraíbles en el nivel de dispositivos, será exclusiva para trabajadores de Auditoría Interna y la Dirección de Informática y Estadística.

10.1.7. Solicitudes adicionales que no se encuentren previstas en el presente documento, deberán ser solicitadas mediante oficio a la Dirección de Informática y Estadística.

[7] Medios extraíbles: son aquellos soportes de almacenamiento diseñados para ser extraídos de la computadora sin tener que apagarla. Ciertos tipos de medios extraíbles están diseñados para ser leídos por lectoras y unidades también extraíbles, permitiendo transportar y respaldar información.

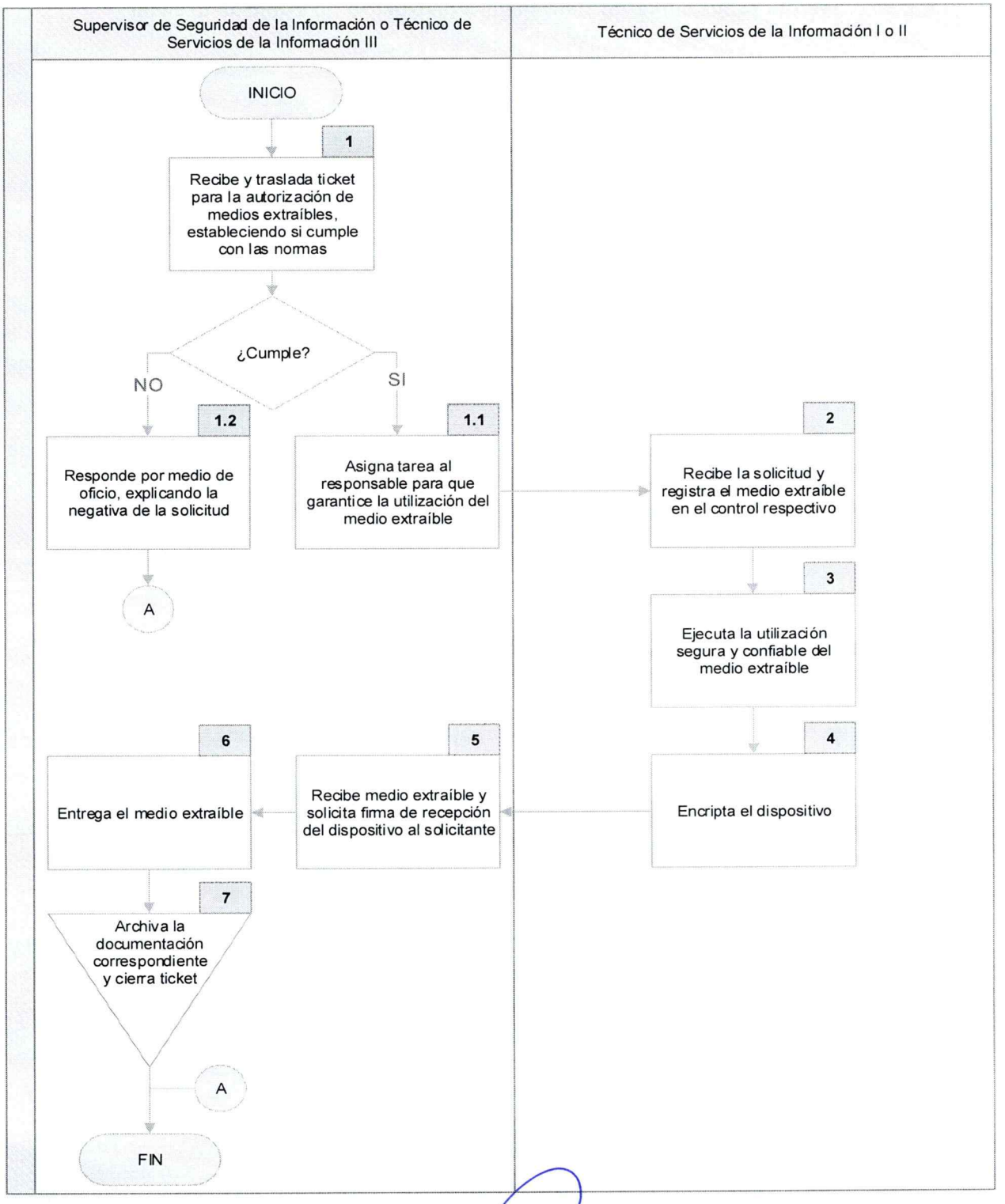
[8] Malware: son amenazas informáticas o software hostil.

10.1.8. Los casos no previstos en el presente procedimiento serán resueltos en su orden por el Jefe de Seguridad Informática, el Subdirector de Servicios Críticos o por el Director de Informática y Estadística.

10.2. Descripción del procedimiento para la autorización de medios extraíbles

Responsable	Paso No.	Actividad
Supervisor de Seguridad de la Información o Técnico de Servicios de la Información III	1.	Recibe y traslada ticket para la autorización de medios extraíbles, estableciendo si cumple con las normas.
	1.1	Si cumple, asigna tarea al responsable para que garantice la utilización del medio extraíble. Continúa en el paso No. 2.
	1.2	No cumple, responde por medio de oficio, explicando la negativa de la solicitud. Fin del procedimiento.
Técnico de Servicios de la Información I o II	2.	Recibe la solicitud y registra el medio extraíble en el control respectivo.
	3.	Ejecuta la utilización segura y confiable del medio extraíble.
	4.	Encripta el dispositivo.
Supervisor de Seguridad de la Información o Técnico de Servicios de la Información III	5.	Recibe medio extraíble y solicita firma de recepción del dispositivo al solicitante.
	6.	Entrega el medio extraíble.
	7.	Archiva la documentación correspondiente y cierra ticket.
		Fin del procedimiento.

10.3. Flujograma del procedimiento para la autorización de medios extraíbles



11. Procedimiento para la administración de equipos firewall

11.1. Normas del procedimiento para la administración de equipos firewall

11.1.1. Únicamente los trabajadores del Departamento de Seguridad Informática designados por el jefe del departamento, podrán tener acceso a la administración de los equipos firewall[9].

11.1.2. Únicamente se dará acceso en el firewall por medio de la "Boleta de acceso políticas de firewall" (ver anexo 6).

11.1.3. Cuando se requiera acceso al firewall por emergencia fuera del horario laboral, se deberá efectuar la solicitud por medio de correo electrónico institucional al Jefe de Seguridad Informática, quien autorizará la configuración de este. La "Boleta de acceso políticas de firewall" deberá entregarse en las primeras horas del día hábil siguiente.

11.1.4. Se otorgarán únicamente los accesos que en la "Boleta de acceso políticas de firewall" estén consignados.

11.1.5. En cada una de las herramientas de administración de los equipos firewall se deberá dejar constancia (en el área de comentarios) de la documentación de respaldo de cada uno de los accesos otorgados.

11.1.6. El acceso requerido se deberá solicitar como mínimo con 2 horas de anticipación.

11.1.7. Únicamente los trabajadores del Departamento de Seguridad Informática podrán consultar las boletas de acceso políticas de firewall originales.

11.1.8. El trabajador designado por el Jefe de Seguridad Informática, para archivar las boletas de acceso políticas de firewall deberá llevar un control de las acciones que se deseen verificar sobre las mismas.

11.1.9. Las boletas de acceso políticas de firewall serán el respaldo de la institución y usuarios por los accesos proporcionados a los sistemas, estás únicamente pueden ser manipuladas por trabajadores del Departamento de Seguridad Informática. A las dependencias fiscalizadoras únicamente se les proporcionará fotocopias simples o fotocopias certificadas de estas, cuando así lo requieran.

[9] Firewall (cortafuegos): sistema o dispositivo capaz de limitar, cifrar y decodificar el tráfico de comunicaciones en una red, impidiendo que usuarios o sistemas no autorizados tengan acceso.

11.1.10. Cuando por motivos de requerimiento de información sea necesario trasladar las boletas de acceso políticas de firewall en original para ser certificadas, se deberá solicitar por medio de oficio en el que se indique quien tendrá la boleta original y el tiempo que necesitará para realizar dicha acción.

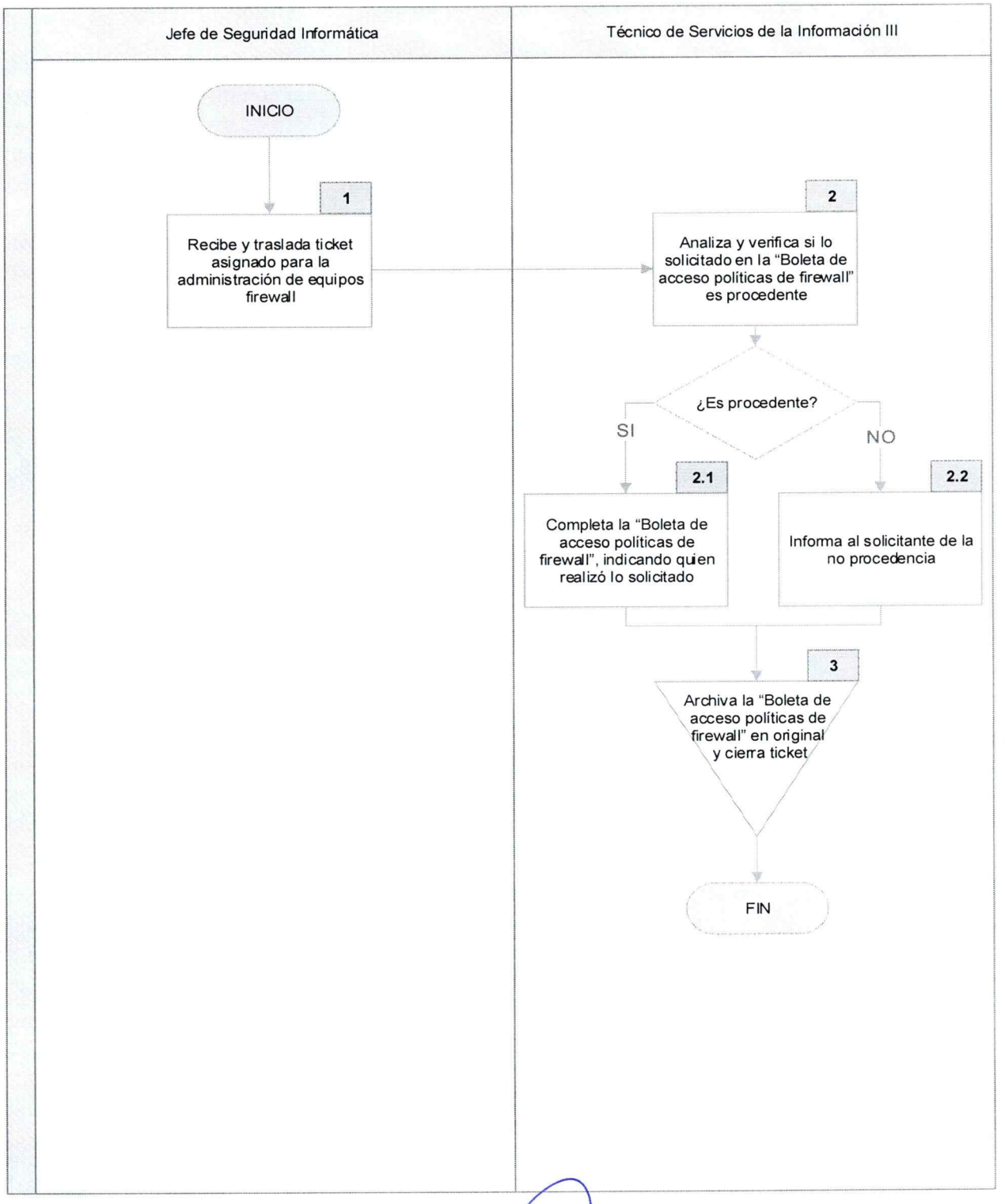
11.1.11. No se podrá realizar ninguna acción con las boletas de acceso políticas de firewall, si no se tiene algún requerimiento oficial que respalde dicha acción.

11.1.12. Los casos no previstos en el presente procedimiento serán resueltos en su orden por el Jefe de Seguridad Informática, el Subdirector de Servicios Críticos o por el Director de Informática y Estadística.

11.2. Descripción del procedimiento para la administración de equipos firewall

Responsable	Paso No.	Actividad
Jefe de Seguridad Informática	1.	Recibe y traslada ticket asignado para la administración de equipos firewall.
Técnico de Servicios de la Información III	2.	Analiza y verifica si lo solicitado en la "Boleta de acceso políticas de firewall" es procedente.
	2.1	Si es procedente, completa la "Boleta de acceso políticas de firewall", indicando quien realizó lo solicitado. Continúa en el paso No. 3.
	2.2	No es procedente, informa al solicitante de la no procedencia. Continúa en el paso No. 3.
	3.	Archiva la "Boleta de acceso políticas de firewall" en original y cierra ticket.
		Fin del procedimiento.

11.3. Flujograma del procedimiento para la administración de equipos firewall



12. Procedimiento para la administración de acceso a internet

12.1. Normas del procedimiento para la administración de acceso a internet

12.1.1. El acceso a internet deberá ser solicitado por medio de la "Boleta única todos los servicios" (ver anexo 1), la cual tendrá que estar completada en su totalidad y autorizada por el jefe inmediato y la máxima autoridad de la oficina ejecutora, dirección administrativa y dependencia de apoyo del Director Ejecutivo, cuando corresponda por el Director Ejecutivo.

12.1.2. Únicamente los trabajadores del Departamento de Seguridad Informática podrán conceder los accesos a internet solicitados por medio de la "Boleta única todos los servicios".

12.1.3. La clasificación de los niveles de perfiles de acceso a internet, según el puesto que se ocupa y actividades, son los siguientes:

NIVEL	SEGMENTO	PERFILES
Básico	Trabajador del área operativa	Acceso a sitios educacionales, médicos, enciclopedias web, blogs personales, banca en línea, buscadores web y seguridad de la información.
Preferente	Trabajador del área operativa	Además de los accesos de nivel básico, sitios de arte y cultura, salud, noticias, sociedad, viajes, folklore, restaurantes, gobierno, tecnología de la información, caridad y estadísticas web.
Jefes	Jefe de departamento	Además de los accesos de nivel básico y preferente, redes sociales, videos, páginas de empleos, educación infantil, y reuniones en línea.
Directores	Directores, Registrador Central de las Personas, Auditor Interno, Inspector General, Secretario General y Comunicador Social	Además de los accesos de nivel básico, preferente y jefes, correo basado en web, radio y tv en línea, compras en línea y web chat.
VIP	Director Ejecutivo, miembros del Directorio y asesores de Dirección Ejecutiva	Además de los accesos a nivel básico, preferente, jefes y directores, almacenamiento en la nube, entretenimiento, mensajería instantánea, servicios de contenidos, sitios de interés general, sitios de acceso remoto.

Cuando se requiera un acceso distinto a servicios, sitios o plataformas establecidos en los perfiles autorizados, se deberá solicitar mediante la "Boleta única todos los servicios" acompañada de un oficio, con las firmas respectivas del jefe inmediato y la máxima autoridad de la oficina ejecutora, dirección administrativa y dependencia de apoyo del Director Ejecutivo, cuando corresponda por el Director Ejecutivo.

12.1.4. Cualquier acceso que no esté considerado dentro de los perfiles definidos, deberá ser analizado individualmente por el Departamento de Seguridad Informática, quien dictaminará sobre la procedencia del otorgamiento del acceso solicitado.

12.1.5. El acceso a internet se proporcionará para ser utilizado como herramienta de trabajo dentro de la institución, haciendo el uso prudente del mismo, evitando propiciar la fuga de información que pueda comprometer y poner en riesgo a la institución.

12.1.6. El acceso a páginas con contenido de o relacionado con armas, drogas, pornografía o que dañen la imagen institucional, queda totalmente restringido.

12.1.7. No está permitido el acceso a páginas con servicios:

a) Almacenamiento en la nube (Dropbox, drive, icloud o similares).
b) Mensajería instantánea (WhatsApp Web, telegram o similares).
c) Alojamiento de videos (youtube, vimeo o similares).
d) Sitios de reproducción de audios (Spotify, Deezer o similares).

De requerir acceso a alguno de los servicios anteriores, la máxima autoridad de las oficinas ejecutoras, direcciones administrativas o dependencias de apoyo del Director Ejecutivo deberá solicitarlo por medio de oficio a la Dirección de Informática y Estadística, siendo estos para fines laborales, no personales. Dichos accesos se asignarán bajo responsabilidad del trabajador asignado.

12.1.8. El Jefe de Seguridad Informática y el Director de Informática y Estadística serán los responsables de autorizar el uso de software para conexiones remotas, mismo deberá utilizarse exclusivamente para fines laborales, no personales.

12.1.9. No está permitido el ingreso a páginas con servicios de correo electrónico personal (Gmail, Yahoo, Hotmail/Outlook), con excepción de autorizaciones especiales solicitadas por medio de oficio por Directorio,

Dirección Ejecutiva o la máxima autoridad de las oficinas ejecutoras, direcciones administrativas o dependencias de apoyo del Director Ejecutivo.

12.1.10. Los accesos concedidos serán notificados por medio de correo electrónico institucional al solicitante, con copia al Jefe de Seguridad Informática

12.1.11. Los accesos a redes inalámbricas deberán de contar con las medidas de seguridad que el Jefe de Seguridad Informática considere necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información.

12.1.12. La creación de nuevas redes inalámbricas se deberá solicitar por medio de oficio con la debida justificación. El Departamento de Seguridad Informática evaluará la solicitud, considerando que se deberá garantizar la seguridad de la información de la institución y la disponibilidad del equipo de acceso a redes inalámbricas.

12.1.13. El Departamento de Seguridad Informática analizará periódicamente si deben eliminarse redes inalámbricas que han dejado de ser utilizadas o que pongan en riesgo la seguridad de la información.

12.1.14. Para que un trabajador pueda tener acceso a internet para las estaciones de trabajo por medio de módems móviles, teléfonos celulares, conexión vía PDA[10] u otros dispositivos inalámbricos, la máxima autoridad de la oficina ejecutora, dirección administrativa o dependencia de apoyo del Director Ejecutivo deberá solicitarlo de forma escrita a la Dirección de Informática y Estadística.

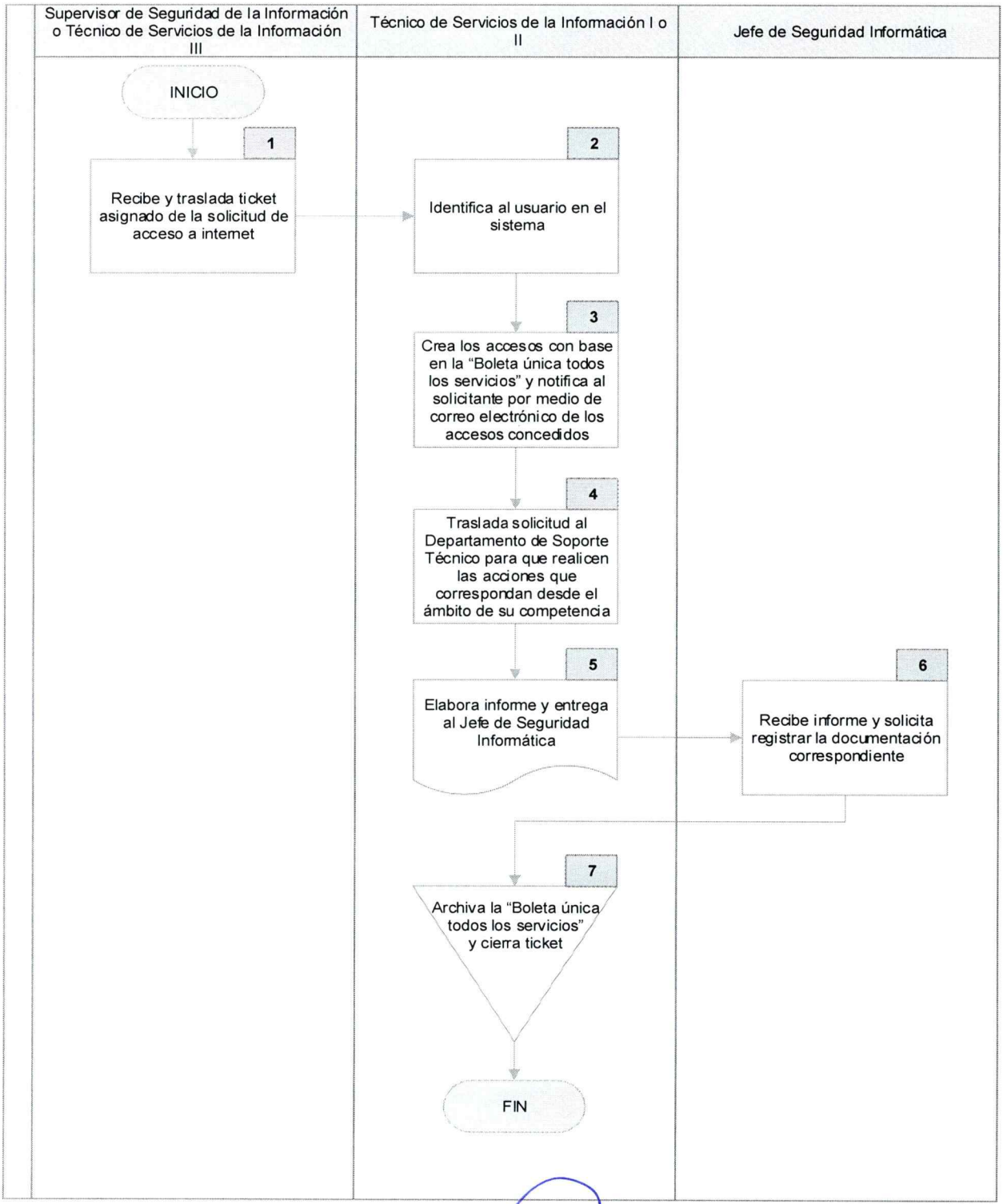
12.1.15. Los casos no previstos en el presente procedimiento serán resueltos en su orden por el Jefe de Seguridad Informática, el Subdirector de Servicios Críticos o por el Director de Informática y Estadística.

[10] Personal Digital Assistant, por sus siglas en inglés PDA (ayudante personal digital): es un dispositivo de pequeño tamaño que combina un ordenador, teléfono/fax, internet y conexiones de red.

12.2. Descripción del procedimiento para la administración de acceso a internet

Responsable	Paso No.	Actividad
Supervisor de Seguridad de la Información o Técnico de Servicios de la Información III	1.	Recibe y traslada ticket asignado de la solicitud de acceso a internet.
Técnico de Servicios de la Información I o II	2.	Identifica al usuario en el sistema.
	3.	Crea los accesos con base en la "Boleta única todos los servicios" y se notifica al solicitante por medio de correo electrónico de los accesos concedidos.
	4.	Traslada solicitud al Departamento de Soporte Técnico para que realicen las acciones que correspondan desde el ámbito de su competencia.
	5.	Elabora informe y entrega al Jefe de Seguridad Informática.
Jefe de Seguridad Informática	6.	Recibe informe y solicita registrar la documentación correspondiente.
Técnico de Servicios de la Información I o II	7.	Archiva la "Boleta única todos los servicios" y cierra ticket.
		Fin del procedimiento.

12.3. Flujograma del procedimiento para la administración de acceso a internet



13. Procedimiento para la actualización de antivirus y antimalware

13.1. Normas del procedimiento para la actualización de antivirus y antimalware

13.1.1. El equipo de cómputo (de escritorio, portátiles y servidores) deberán tener instalado el antivirus autorizado por la Dirección de Informática y Estadística.

13.1.2. El equipo de cómputo que sea configurado por primera vez a la red del RENAP se le deberá instalar el software de antivirus y antimalware.

13.1.3. La instalación del antivirus y antimalware en los servidores se realizará de forma manual por el Departamento de Seguridad Informática.

13.1.4. La administración del servidor del software de antivirus y antimalware estará a cargo del Departamento de Seguridad Informática, por lo que es responsable de mantener contratos vigentes de protección contra virus y malware.

13.1.5. Las contraseñas de licenciamiento del antivirus y antimalware son administradas únicamente por el Departamento de Seguridad Informática, quien configurará la consola y establecerá los tiempos de actualización de acuerdo con la licencia vigente.

13.1.6. Las actualizaciones se realizarán automáticamente por medio de un servidor donde estará instalada la consola principal de antivirus, en el cual se establecerá el horario de actualización. Las actualizaciones que no sean automáticas serán efectuadas por el Departamento de Seguridad Informática.

13.1.7. El trabajador encargado de la actualización generará un informe mensual de la cantidad de equipos actualizados, el cual deberá ser presentado ante el Jefe de Seguridad Informática con copia al Director de Informática y Estadística.

13.1.8. El equipo de cómputo que no cumpla con los requisitos mínimos de instalación del antivirus será desconectado y excluido de la red del RENAP, para evitar riesgos de infección en otros equipos de cómputo.

13.1.9. Las configuraciones de las reglas del antivirus son creadas por trabajadores del Departamento de Seguridad Informática, quienes deberán considerar el criterio de cada departamento de la Dirección de Informática y Estadística.

13.1.10. Está prohibida la instalación de otros tipos de antivirus que no sean los establecidos por la Dirección de Informática y Estadística.

13.1.11. Queda prohibido cambiar la configuración o parámetros de los equipos de cómputo, sistemas operativos o aplicaciones de la institución. Dicho procedimiento deberá realizarlo el trabajador autorizado de la Dirección de Informática y Estadística.

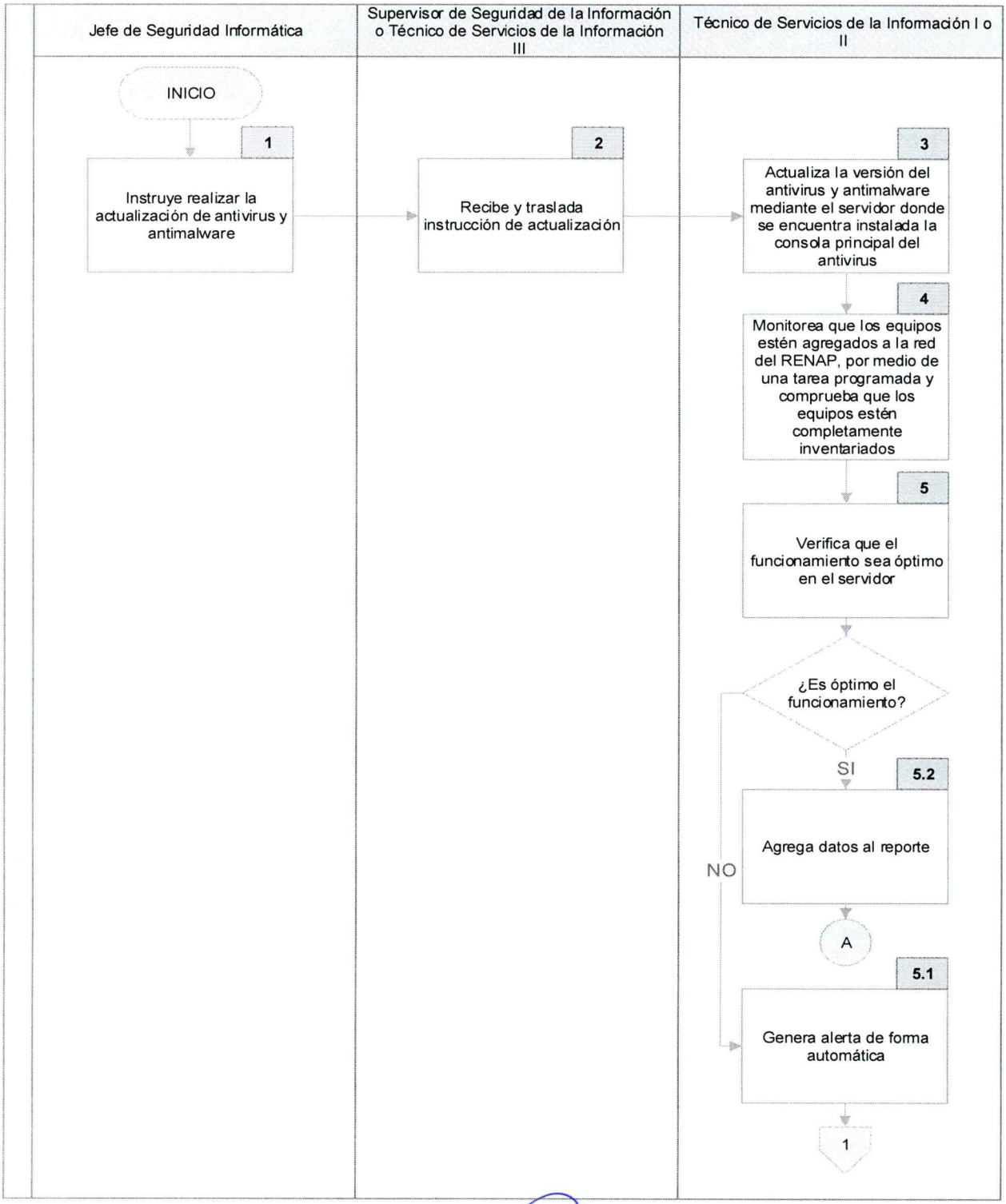
13.1.12. El Departamento de Seguridad Informática deberá llevar el control de la cantidad de licencias instaladas del software de antivirus y antimalware.

13.1.13. Los casos no previstos en el presente procedimiento serán resueltos en su orden por el Jefe de Seguridad Informática, el Subdirector de Servicios Críticos o por el Director de Informática y Estadística.

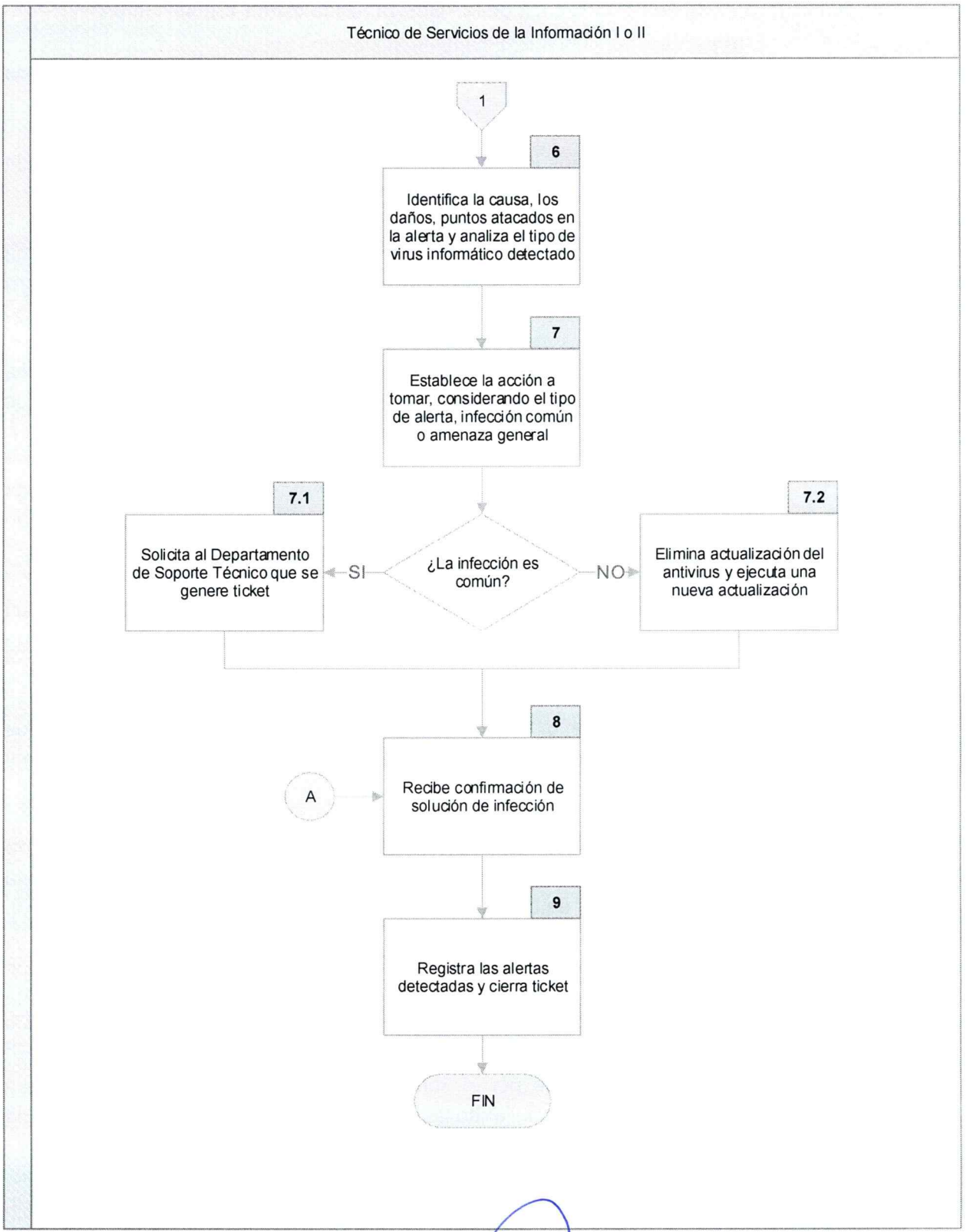
13.2. Descripción del procedimiento para la actualización de antivirus y antimalware

Responsable	Paso No.	Actividad
Jefe de Seguridad Informática	1.	Instruye realizar la actualización de antivirus y antimalware.
Supervisor de Seguridad de la Información o Técnico de Servicios de la Información III	2.	Recibe y traslada instrucción de actualización.
Técnico de Servicios de la Información I o II	3.	Actualiza la versión del antivirus y antimalware mediante el servidor donde se encuentra instalada la consola principal del antivirus.
	4.	Monitorea que los equipos estén agregados a la red del RENAP, por medio de una tarea programada y comprueba que los equipos estén completamente inventariados.
	5.	Verifica que el funcionamiento sea óptimo en el servidor.
	5.1	El funcionamiento no es óptimo, genera alerta de forma automática. Continúa en el paso No. 6.
	5.2	El funcionamiento es óptimo, agrega datos al reporte. Continúa en el paso No. 8.
	6.	Identifica la causa, los daños, puntos atacados en la alerta y analiza el tipo de virus informático detectado.
	7.	Establece la acción a tomar, considerando el tipo de alerta, infección común o amenaza general.
	7.1	La infección es común, solicita al Departamento de Soporte Técnico que se genere ticket. Continúa en el paso No. 8.
	7.2	La infección no es común, elimina actualización del antivirus y ejecuta una nueva actualización. Continúa en el paso No. 8.
	8.	Recibe confirmación de solución de infección.
	9.	Registra las alertas detectadas y cierra ticket.
		Fin del procedimiento.

13.3. Flujograma del procedimiento para la actualización de antivirus y antimalware



Elaborado por:	Revisado por:	Revisado por:	Validado por:	Validado por:	Aprobado por:
Departamento de Organización y Métodos	Jefe de Organización y Métodos	Director de Gestión y Control Interno	Subdirector de Servicios Críticos	Director de Informática y Estadística	Director Ejecutivo



Elaborado por:	Revisado por:	Revisado por:	Validado por:	Validado por:	Aprobado por:
Departamento de Organización y Métodos	Jefe de Organización y Métodos	Director de Gestión y Control Interno	Subdirector de Servicios Críticos	Director de Informática y Estadística	Director Ejecutivo

14. Procedimiento para la administración de la "Boleta única todos los servicios"

14.1. Normas del procedimiento para la administración de la "Boleta única todos los servicios"

14.1.1. La "Boleta única todos los servicios" (ver anexo 1) será recibida y archivada por el Departamento de Seguridad Informática.

14.1.2. La "Boleta única todos los servicios" deberá completarse desde la página https://pointer.renap.gob.gt e imprimir la misma para trasladarla de manera oficial a la Dirección de Informática y Estadística.

14.1.3. Toda "Boleta única todos los servicios" al ingresar a la Dirección de Informática y Estadística deberá estar foliada y archivada según especifique el Jefe de Seguridad Informática.

14.1.4. Únicamente los trabajadores del Departamento de Seguridad Informática podrán consultar las boletas únicas todos los servicios originales que han ingresado, a excepción de lo dispuesto en la norma 14.1.7.

14.1.5. El trabajador designado por el Jefe de Seguridad Informática deberá llevar un control y seguimiento de las acciones y accesos solicitados por medio de la "Boleta única todos los servicios".

14.1.6. La fotocopia simple o fotocopia certificada de la "Boleta única todos los servicios", será solicitada por medio de oficio a la Dirección de Informática y Estadística.

14.1.7. La "Boleta única todos los servicios" podrá ser proporcionada a Secretaría General para que sea certificada una fotocopia, cuando previamente se haya solicitado por medio de oficio.

14.1.8. No se podrá realizar ninguna acción consignada en las boletas únicas todos los servicios, si no se tiene algún requerimiento oficial que respalde dicha acción.

14.1.9. El trabajador designado por el Jefe de Seguridad Informática realizará las acciones necesarias cumpliendo las especificaciones de la "Boleta única todos los servicios", según área de experiencia y complejidad de lo requerido.

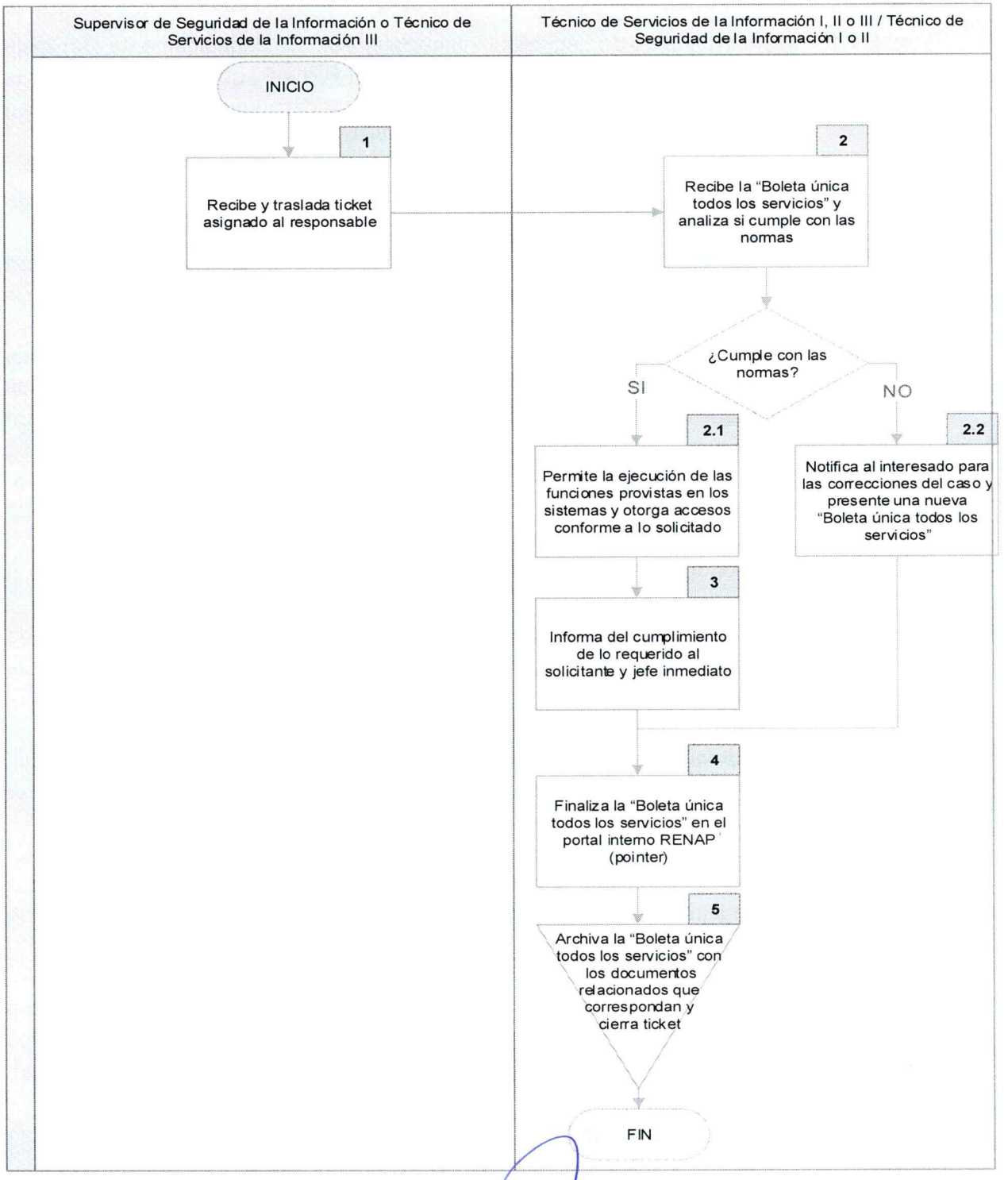
14.1.10. Cuando sean accesos que no corresponden al perfil del puesto del solicitante, se deberá adjuntar la "Boleta única todos los servicios", oficio que justifique el uso que se les dará a los accesos requeridos, el cual deberá ser firmado y sellado por la máxima autoridad de la oficina ejecutora, dirección administrativa o dependencia de apoyo del Director Ejecutivo.

14.1.11. Los casos no previstos en el presente procedimiento serán resueltos en su orden por el Jefe de Seguridad Informática, el Subdirector de Servicios Críticos o por el Director de Informática y Estadística.

14.2. Descripción del procedimiento para la administración de la "Boleta única todos los servicios"

Responsable	Paso No.	Actividad
Supervisor de Seguridad de la Información o Técnico de Servicios de la Información III	1.	Recibe y traslada ticket asignado al responsable.
Técnico de Servicios de la Información I, II o III / Técnico de Seguridad de la Información I o II	2.	Recibe la "Boleta única todos los servicios" y analiza si cumple con las normas.
	2.1	Si cumple con las normas, permite la ejecución de las funciones provistas en los sistemas y otorga accesos conforme a lo solicitado. Continúa en el paso No. 3.
	2.2	No cumple con las normas, notifica al interesado para las correcciones del caso y presente una nueva "Boleta única todos los servicios". Continúa en el paso No. 4.
	3.	Informa del cumplimiento de lo requerido al solicitante y jefe inmediato.
	4.	Finaliza la "Boleta única todos los servicios" en el portal interno RENAP (pointer).
	5.	Archiva la "Boleta única todos los servicios" con los documentos relacionados que correspondan y cierra ticket.
		Fin del procedimiento.

14.3. Flujograma del procedimiento para la administración de la "Boleta única todos los servicios"



15. Procedimiento para análisis de vulnerabilidades

15.1. Normas del procedimiento para análisis de vulnerabilidades

15.1.1. El Departamento de Seguridad Informática realizará periódicamente el análisis de vulnerabilidades a las dependencias del RENAP, que tengan que ver de forma directa o indirecta con aspectos de seguridad informática y de seguridad de la información.

15.1.2. El Departamento de Seguridad Informática realizará el análisis de vulnerabilidades, acorde a las condiciones siguientes:

a) Cuando lo considere pertinente realizará el análisis de seguridad informática generando los reportes de las vulnerabilidades para entregar a las áreas evaluadas de ser necesario.
b) De forma selectiva en todas las dependencias del RENAP, quienes deberán entregar informe de las vulnerabilidades encontradas en los casos que se crean pertinentes a los directores de las dependencias para su respectiva mitigación.
c) Bajo demanda de la máxima autoridad de las oficinas ejecutoras, direcciones administrativas y dependencias de apoyo del Director Ejecutivo, o bien, subdirectores.
d) Cronograma previamente establecido.

15.1.3. El Departamento de Seguridad Informática luego de realizar el análisis de vulnerabilidades categorizará las debilidades con base al impacto de la amenaza.

15.1.4. El Departamento de Seguridad Informática realizará un documento en el cual se describan las sugerencias y recomendaciones para minimizar o erradicar las vulnerabilidades encontradas, tales como:

a) Recomendaciones de parchados[11].
b) Medidas de seguridad a implementar.
c) Seguimiento a instalaciones de software y hardware según políticas de seguridad.

15.1.5. El Jefe de Seguridad Informática deberá trasladar a través del medio oficial con visto bueno del Subdirector de Servicios Críticos y Director de Informática y Estadística los casos que correspondan a cada departamento mitigar, explicando los hallazgos encontrados.

[11] Parchados: cambios que se aplican a un programa para corregir errores, agregarle funcionalidad, actualizarlo, entre otros.

15.1.6. Conforme a la criticidad de los hallazgos encontrados, el Departamento de Seguridad Informática establecerá tiempos de respuesta y solicitará a la dependencia analizada el reporte de las acciones que tomó para la mitigación de las vulnerabilidades. El resultado exitoso de las acciones de mitigación permitirá realizar nuevamente el análisis de vulnerabilidad en la dependencia.

15.1.7. Cuando la vulnerabilidad encontrada en el análisis o prueba respectiva no pueda ser mitigada por cualquier razón, deberá ser debidamente justificada por medio de oficio con copia al Departamento de Seguridad Informática, indicando los argumentos y la vulnerabilidad a la que se refiere, comprometiéndose a buscar alternativas; aunado a lo anterior, se podrá solicitar a la Dirección de Informática y Estadística el apoyo para mitigar las vulnerabilidades encontradas.

15.1.8. La ejecución de las acciones que den solución definitiva a las vulnerabilidades encontradas a través del análisis o prueba, quedan estrictamente delegadas al departamento responsable de los equipos y sistemas a los cuales se les realizó análisis.

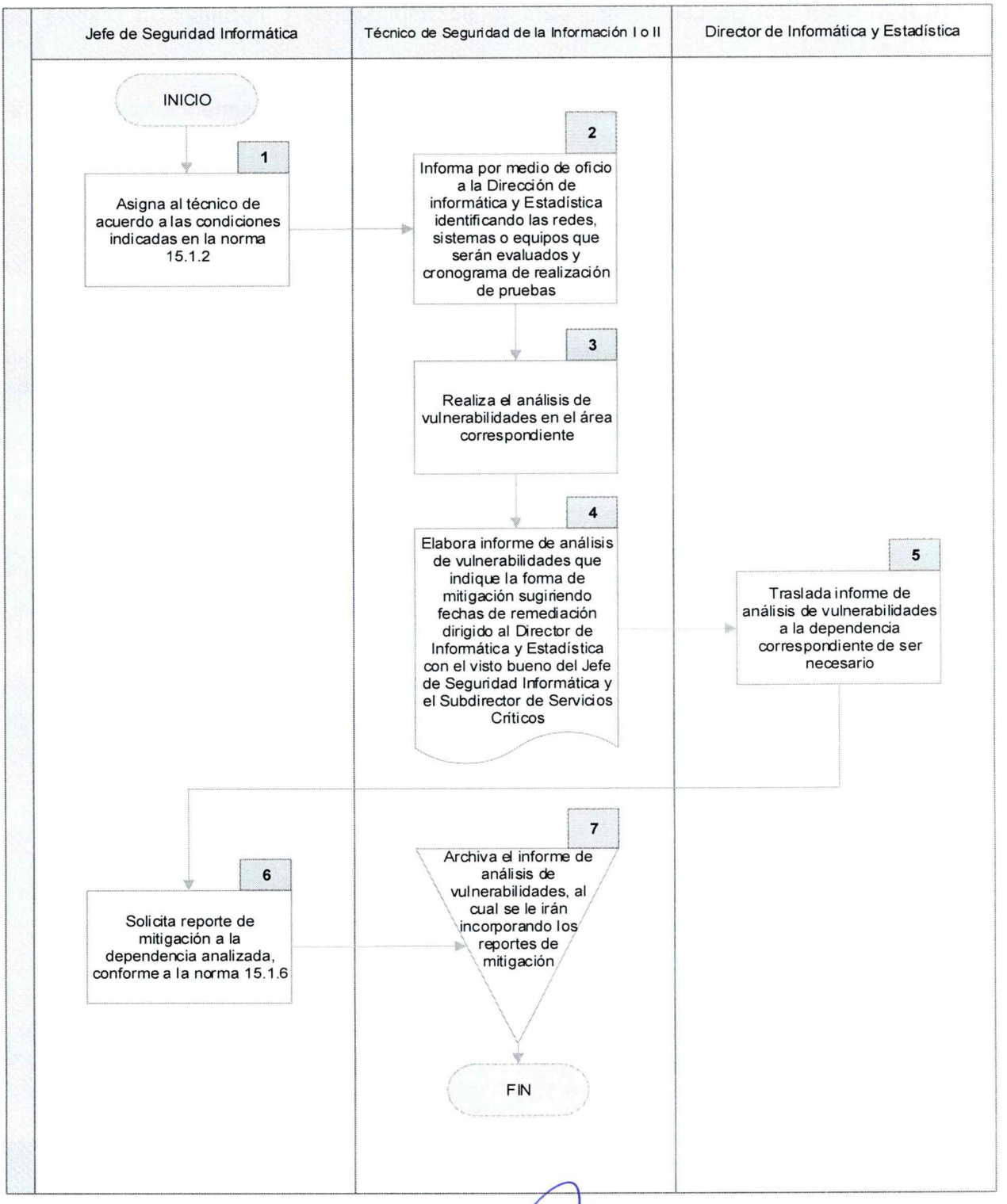
15.1.9. Los resultados e informes del análisis por contener información sensible deberán ser administrados únicamente por la Dirección de Informática y Estadística, a través del Departamento de Seguridad Informática y a quien este delegue las acciones para la mitigación de las vulnerabilidades encontradas.

15.1.10. Los casos no previstos en el presente procedimiento serán resueltos en su orden por el Jefe de Seguridad Informática, el Subdirector de Servicios Críticos o por el Director de Informática y Estadística.

15.2. Descripción del procedimiento para análisis de vulnerabilidades

Responsable	Paso No.	Actividad
Jefe de Seguridad Informática	1.	Asigna al técnico de acuerdo con las condiciones indicadas en la norma 15.1.2.
Técnico de Seguridad de la Información I o II	2.	Informa por medio de oficio a la Dirección de informática y Estadística identificando las redes, sistemas o equipos que serán evaluados y cronograma de realización de pruebas.
	3.	Realiza el análisis de vulnerabilidades en el área correspondiente.
	4.	Elabora informe de análisis de vulnerabilidades que indique la forma de mitigación sugiriendo fechas de remediación dirigido al Director de Informática y Estadística con el visto bueno del Jefe de Seguridad Informática y el Subdirector de Servicios Críticos.
Director de Informática y Estadística	5.	Traslada informe de análisis de vulnerabilidades a la dependencia correspondiente de ser necesario.
Jefe de Seguridad Informática	6.	Solicita reporte de mitigación a la dependencia analizada, conforme a la norma 15.1.6.
Técnico de Seguridad de la Información I o II	7.	Archiva el informe de análisis de vulnerabilidades, al cual se le irán incorporando los reportes de mitigación.
		Fin del procedimiento.

15.3. Flujograma del procedimiento para análisis de vulnerabilidades



16. Procedimiento para la deshabilitación y habilitación masiva de accesos

16.1. Normas del procedimiento para la deshabilitación y habilitación masiva de accesos

16.1.1. Al final de cada año, la Subdirección de Recursos Humanos trasladará a la Dirección de Informática y Estadística, la información de las personas que no tendrán contrato laboral para el año siguiente.

16.1.2. El Departamento de Seguridad Informática procederá con la respectiva deshabilitación de accesos a los servicios informáticos, a los usuarios que no tendrán contrato laboral para el siguiente año.

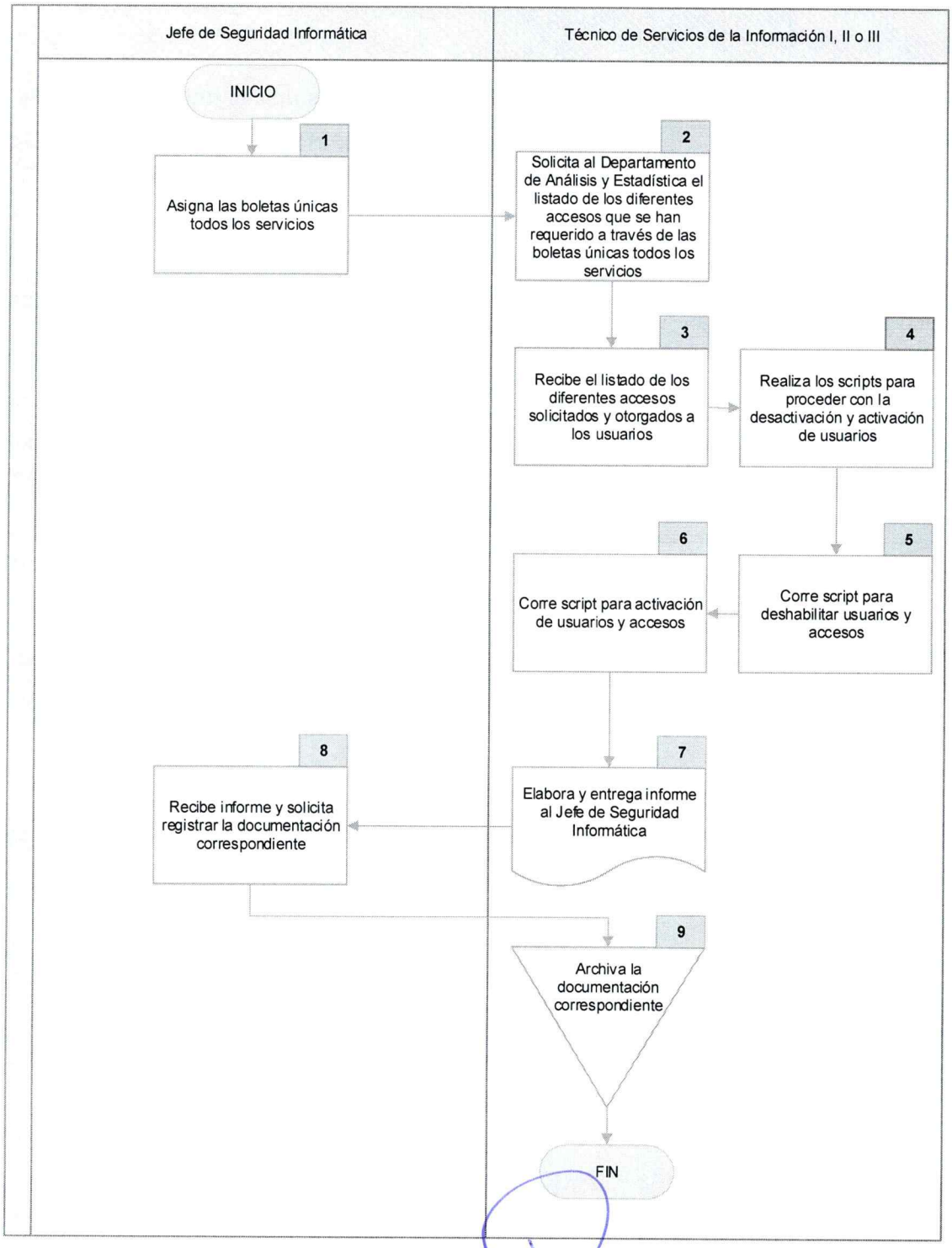
16.1.3. Los casos no previstos en el presente procedimiento serán resueltos en su orden por el Jefe de Seguridad Informática, el Subdirector de Servicios Críticos o por el Director de Informática y Estadística.

16.2. Descripción del procedimiento para la deshabilitación y habilitación masiva de accesos

Responsable	Paso No.	Actividad
Jefe de Seguridad Informática	1.	Asigna las boletas únicas todos los servicios.
Técnico de Servicios de la Información I, II o III	2.	Solicita al Departamento de Análisis y Estadística el listado de los diferentes accesos que se han requerido a través de las boletas únicas todos los servicios.
	3.	Recibe el listado de los diferentes accesos solicitados y otorgados a los usuarios.
	4.	Realiza los scripts para proceder con la desactivación y activación de usuarios.
	5.	Corre script[12] para deshabilitar usuarios y accesos.
	6.	Corre script para activación de usuarios y accesos.
	7.	Elabora y entrega informe al Jefe de Seguridad Informática.
Jefe de Seguridad Informática	8.	Recibe informe y solicita registrar la documentación correspondiente.
Técnico de Servicios de la Información I, II o III	9.	Archiva la documentación correspondiente.
		Fin del procedimiento.

[12] Script: es un lenguaje de programación que ejecuta diversas funciones en el interior de un programa de computador.

16.3. Flujograma del procedimiento para la deshabilitación y habilitación masiva de accesos



17. Procedimiento para la deshabilitación de accesos a la red y servicios institucionales asociados por inactividad

17.1. Normas del procedimiento para la deshabilitación de accesos a la red y servicios institucionales asociados por inactividad

17.1.1. El Departamento de Seguridad Informática procederá a deshabilitar a los usuarios que estén inactivos por más de cinco días laborables.

17.1.2. El Departamento de Seguridad Informática elaborará y entregará a la Subdirección de Recursos Humanos el consolidado mensual de usuarios deshabilitados con visto bueno del Jefe de Seguridad Informática en los primeros tres días hábiles del mes siguiente.

17.1.3. Para habilitar nuevamente el acceso a la red y servicios institucionales asociados, estos deberán ser solicitados por medio de la "Boleta única todos los servicios" (ver anexo 1), la cual tendrá que ser completada en su totalidad y autorizada por el jefe inmediato y la máxima autoridad de la oficina ejecutora, dirección administrativa o dependencia de apoyo del Director Ejecutivo, cuando corresponda por el Director Ejecutivo.

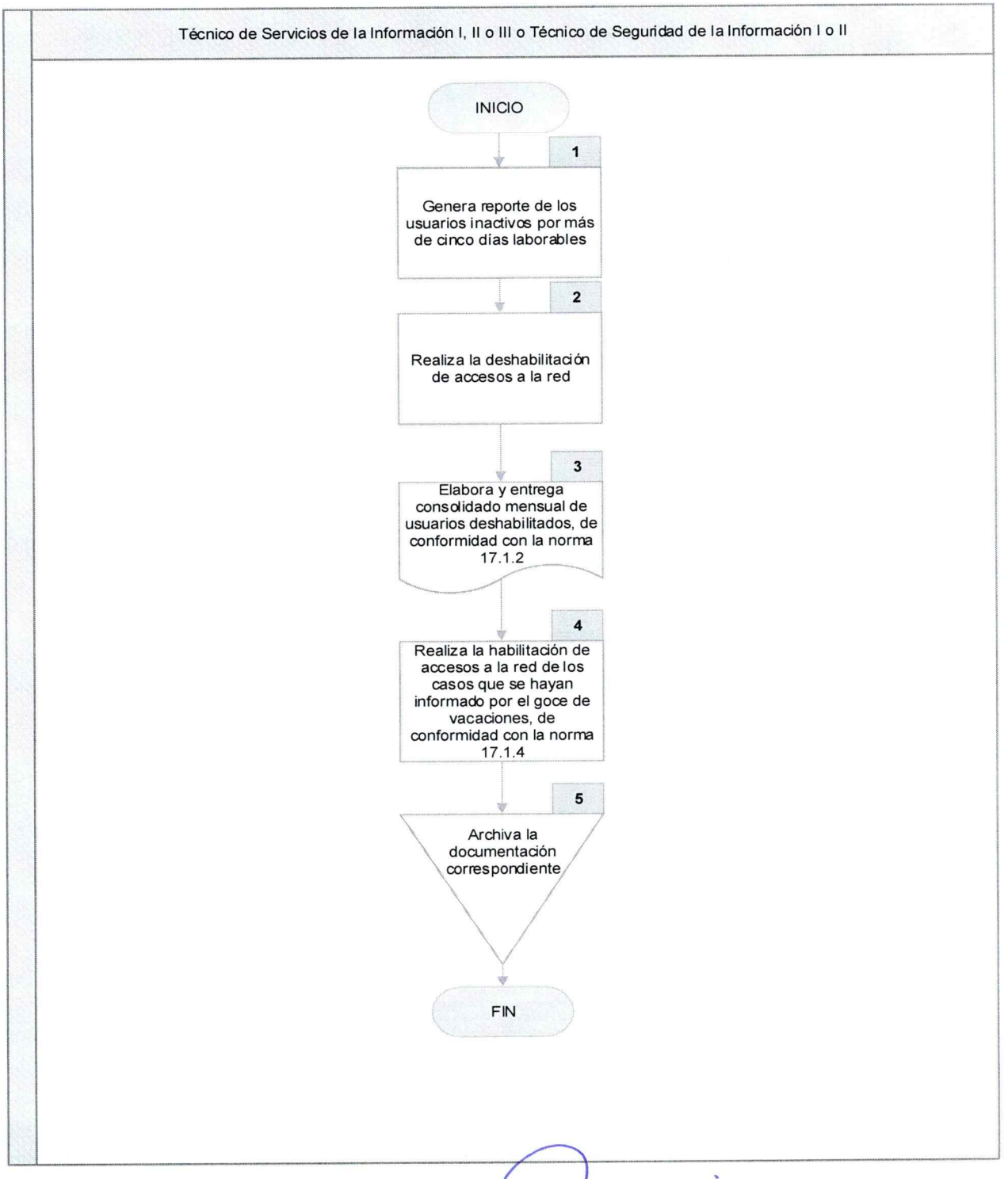
17.1.4. Se podrá dispensar de presentar la "Boleta única todos los servicios" cuando la deshabilitación haya derivado por el goce de vacaciones del trabajador, para lo cual la máxima autoridad de la oficina ejecutora, dirección administrativa o dependencia de apoyo del Director Ejecutivo deberá informar por medio del oficio a la Dirección de Informática y Estadística la fecha en la que el trabajador retornará de su período vacacional.

17.1.5. Los casos no previstos en el presente procedimiento serán resueltos en su orden por el Jefe de Seguridad Informática, el Subdirector de Servicios Críticos o por el Director de Informática y Estadística.

17.2. Descripción del procedimiento para la deshabilitación de accesos a la red y servicios institucionales asociados por inactividad

Responsable	Paso No.	Actividad
Técnico de Servicios de la Información I, II o III o Técnico de Seguridad de la Información I o II	1	Genera reporte de los usuarios inactivos por más de cinco días laborables.
	2	Realiza la deshabilitación de accesos a la red.
	3	Elabora y entrega consolidado mensual de usuarios deshabilitados, de conformidad con la norma 17.1.2.
	4	Realiza la habilitación de accesos a la red de los casos que se hayan informado por el goce de vacaciones, de conformidad con la norma 17.1.4.
	5	Archiva la documentación correspondiente.
		Fin del procedimiento.

17.3. Flujograma del procedimiento para la deshabilitación de accesos a la red y servicios institucionales asociados por inactividad



Elaborado por:	Revisado por:	Revisado por:	Validado por:	Validado por:	Aprobado por:
Departamento de Organización y Métodos	Jefe de Organización y Métodos	Director de Gestión y Control Interno	Subdirector de Servicios Críticos	Director de Informática y Estadística	Director Ejecutivo

Anexo 1. Boleta única todos los servicios

RENAP	DIRECCIÓN DE INFORMÁTICA Y ESTADÍSTICA - RENAP - BOLETA ÚNICA TODOS LOS SERVICIOS	RENAP Registro Nacional de las Personas
FO-DI-45		
Edición: **00-00-0000**		

Imprimir a doble cara

No.**000-0-0000**

Fecha:	**CUI:**	**Código empleado:**	**Oficina Registral No.**
Nombre completo:			
Unidad Administrativa y Departamento al que pertenece:		**Departamento, Municipio:**	
Puesto:		**Télefono/Extensión:**	**Sede:**
Motivo de Solicitud:	**Tipo equipo:**	**Fecha inicio:**	**Fecha fin:**
IP:	**Nombre de equipo:**	**No. Inventario de equipo**	
Activación	**Otros (especifique)**		

Al trabajador/**contratista** de RENAP se le hace entrega del usuario y contraseña de red para la conexión al dominio central denominado RENAP.LOCAL, habilitación de VPN, acceso al aplicativo de Consulta de DPI y/o usuario de SIRECI por lo tanto es el único responsable del uso que le dé. Cualquier anomalía causada por el mal uso o divulgación, se suspenderá indefinidamente de la red, se le deducirán responsabilidades previstas en los documentos normativos vigentes a la fecha del hecho, así como la responsabilidad civil y/o penal que del mismo se derive.

ACCESOS	CREAR	MODIFICAR	BAJA	PERFIL
USUARIO DE RED				

* Con excepción de personal temporal 029.
** Únicamente para accesos al Sistema de Registro Civil de las Personas -SIRECI-

Firma y nombre del Usuario	*Autorizado por Jefe inmediato o Registrador Civil (firma, nombre y sello)	Autorizado por Director de Área (firma, nombre y sello)	**Autorización de Registrador Central de las Personas o Subdirector de Registro Central de las Personas (Firma, nombre y sello)

TÉRMINOS Y CONDICIONES

El presente documento hace de su conocimiento sobre la responsabilidad adquirida por el trabajador/contratista al momento de tener acceso a la red del RENAP, SIRECI, Intranet, Consulta DPI o acceso a VPN, siendo este último utilizado para llevar un mejor servicio a los lugares que no tienen una conexión, por lo tanto, los siguientes términos y condiciones deben de ser leídos y aceptados.

1. La cuenta de acceso y la contraseña, el usuario de red, SIRECI y/o Intranet es PERSONAL E INTRANSFERIBLE. La responsabilidad contraída por el trabajador/contratista inicia con su primer ingreso al dominio de RENAP y los sistemas a los que tendrá acceso en la Consulta DPI de RENAP.
2. La Dirección de Informática y Estadística brinda la contraseña para ingresar por primera vez a la red, misma que deberá ser cambiada por el trabajador/contratista en ese momento por ser un proceso automático requerido por el sistema. De allí en adelante, las contraseñas del trabajador/contratista serán administradas bajo responsabilidad única del trabajador/contratista, ya que, por políticas de seguridad, el sistema obliga que sean cambiadas cada 60 días, por lo que la Dirección de Informática y Estadística NO tiene conocimiento de las mismas.
3. La contraseña deberá cumplir con ciertas características de las mejores prácticas, como lo son: poseer una letra mayúscula, números, letras y un carácter especial, la longitud de la contraseña será de 8 caracteres mínimo (ejemplo de contraseña de red "Ejemplo%2*4").
4. Si en algún momento se detecta que el trabajador/contratista violó la seguridad se procederá a tomar medidas disciplinarias según el Reglamento Interno de Trabajo del Registro Nacional de las Personas -RENAP-. El Departamento de Seguridad Informática deberá deshabilitar inmediatamente el acceso del trabajador/contratista de la red central del Registro Nacional de las Personas -RENAP-.
5. Si se detecta que el trabajador/contratista mediante el usuario asignado (Red, Correo Electrónico, SIRECI, Intranet, Consulta DPI), ha realizado la posible comisión de un hecho ilícito, el mismo será responsable de conformidad a los documentos normativos vigentes a la fecha del hecho y la legislación aplicable.
6. El trabajador/contratista no deberá por ningún motivo realizar actividades encaminadas a violar la seguridad de los servicios y sistemas utilizados en el RENAP, como también el intento o acceso a la información sin estar acreditado dentro del registro de usuarios en el directorio activo de RENAP.
7. El correo electrónico institucional deberá ser utilizado única y exclusivamente para el intercambio de información relacionada con asuntos de trabajo y para el cumplimiento de los propósitos de la Institución, no para uso personal. Está prohibido el uso del correo electrónico para envío, reenvío o respuesta de correos con archivos adjuntos de un tamaño mayor al designado según el perfil de correo asignado al usuario.
8. Está prohibido el envío de los archivos de música, video, animación, chistes, mensajes en cadenas, lenguaje soez y/o pornografías por medio del correo electrónico institucional.

Elaborado por:	Revisado por:	Revisado por:	Validado por:	Validado por:	Aprobado por:
Departamento de Organización y Métodos	Jefe de Organización y Métodos	Director de Gestión y Control Interno	Subdirector de Servicios Críticos	Director de Informática y Estadística	Director Ejecutivo

RENAP	DIRECCIÓN DE INFORMÁTICA Y ESTADÍSTICA - RENAP - BOLETA ÚNICA TODOS LOS SERVICIOS	RENAP Registro Nacional de las Personas
FO-DI-45		
Edición: **00-00-0000**		

Imprimir a doble cara

No.**000-0-0000**

9. Se prohíbe el almacenamiento de imágenes, música y todo archivo que no esté relacionado a las actividades del RENAP y que afecten el buen funcionamiento del equipo, se podrán eliminar por el personal de la Subdirección de Servicios Críticos de la Dirección de Informática y Estadística, sin previa autorización. Se procederá a levantar un acta de conocimiento en donde se describe las faltas cometidas como también el tipo de archivo(s) eliminado(s). Toda información que se encuentra en los equipos de computo (de escritorio o laptop) ES PROPIEDAD DEL REGISTRO NACIONAL DE LAS PERSONAS -RENAP-, por lo tanto, está prohibida la sustracción, divulgación, cambio o copia de la misma.
10. La Dirección de Informática y Estadística es la única autorizada para proporcionar el acceso los usuarios de Red, Internet, Correo Electrónico, SIRECI, Intranet, Consulta DPI y acceso a VPN.
11. El trabajador/contratista deberá notificar en forma inmediata a la Dirección de Informática y Estadística si detecta el uso indebido o no autorizado de su cuenta por terceras personas.
12. El trabajador/contratista deberá de indicar los accesos a consultar para la aplicación de Consulta DPI, la Dirección de Informática y Estadística evaluará el nivel de acceso solicitado.
13. El trabajador/contratista está sujeto a auditorias en cualquier momento y sin previo aviso que realice la Dirección de Informática y Estadística.
14. El trabajador/contratista es el único responsable del uso que se le dé al usuario asignado, cualquier anomalía causada por el mal uso, divulgación de la información, se suspenderá indefinidamente de la red y se enviará copia del informe a su Dirección para que se proceda según el régimen disciplinario establecido en el Reglamento Interno de Trabajo del RENAP.
15. El trabajador/contratista que firma el presente documento es responsable del usuario y contraseña que se le proporciona para su conexión y se deducirán por la vía correspondiente la responsabilidad civil y/o penal que del mal uso o divulgación se deriven.
16. Toda la información creada, copiada, transportada, procesada dentro de este acceso es propiedad exclusiva del Registro Nacional de las Personas -RENAP-.
17. Al trabajador/contratista que a requerimiento se le hace entrega del usuario y contraseña de VPN para la conexión a la central de RENAP, siendo el único responsable del uso que se le dé a este.
18. Para poder brindar perfil y accesos a SIRECI e Intranet se debe adjuntar a esta solicitud copia de nombramiento de la persona, por parte de la Subdirección de Recursos Humanos.
19. El trabajador/contratista no deberá por ningún motivo realizar actividades encaminadas a violar la seguridad de los servicios y sistemas utilizados en el RENAP, como también el intento o acceso a la información sin estar acreditado dentro del registro de usuarios de los sistemas.
20. No está autorizado que el trabajador/contratista obtenga internet por medio de módems móviles, teléfonos celulares, conexión vía PDA, USB, Claro, Tigo, Movistar u otros dispositivos inalámbricos que no sean autorizados por la Dirección de Informática y Estadística.
21. El Servicio de internet es una herramienta exclusiva para actividades de trabajo. Está estrictamente prohibido cualquier uso con fines comerciales, políticos, particulares o cualquier otro que no sea laboral.
22. El trabajador/contratista si no tiene acceso autorizado no podrá acceder a páginas con correo electrónico que no sean del RENAP. Ejemplo Hotmail, Yahoo, Gmail.
23. Los trabajador/contratistas no deberán descargar y/o instalar ningún tipo de software sin la autorización de la Dirección de Informática y Estadística, aunque este sea gratuito.
24. Cada usuario tendrá acceso al servicio de internet según el rol que le corresponda (Director, Jefe y Usuario).
25. La Dirección de Informática y Estadística es el encargado de realizar la baja definitivamente del usuario en los sistemas, siempre y cuando se haga llegar el formulario con firmas y sello del jefe inmediato (si aplica), y/o el correo electrónico por parte de la Subdirección de Recursos Humanos con la información de las personas que terminaron su relación laboral.
26. El uso de SIRECI y Consulta DPI deberán utilizarse única y exclusivamente para asuntos de trabajo y para el cumplimiento de los propósitos de la Institución, no para uso personal.
27. Toda información que se encuentra dentro del Sistema SIRECI y Consulta DPI es PROPIEDAD DEL REGISTRO NACIONAL DE LAS PERSONAS -RENAP-, por lo tanto, está prohibida la sustracción, divulgación, cambio o copia de la misma. Se deducirán por la vía correspondiente la responsabilidad civil y/o penal que del mal uso o divulgación se deriven.
28. El trabajador/contratista deberá bloquear el equipo cuando se retire de su lugar para evitar que cualquier persona pueda tener acceso al sistema utilizando su usuario y pueda hacer mal uso del mismo.
29. Si tiene problema con el ingreso de su contraseña llame a Help Desk, extensión 1910 en donde se le estará brindando el apoyo necesario.
30. Para crear el usuario de SIRECI y/o Intranet, debe estar creado previamente el usuario de red.
31. Para el acceso a SIRECI e Intranet, el usuario y contraseña son las mismas utilizadas para tener acceso a la red del -RENAP-.
32. Registro Central de las Personas será el encargado de autorizar los permisos para los accesos del Sistema de Registro Civil -SIRECI-.
33. La información obtenida a través de los links autorizados es única y exclusivamente responsabilidad del trabajador/contratista y por ningún motivo deberá compartirla por ningún medio.

El trabajador/contratista declara haber leído y aceptado íntegramente los términos y condiciones.

Nombre Completo: Firma:_____

Acceso	Día:	Mes:	Año:	Hora:	Operado por:	Perfil Asignado
USUARIO DE RED						
ASIGNACIÓN DE EQUIPO						

Elaborado por:	Revisado por:	Revisado por:	Validado por:	Validado por:	Aprobado por:
Departamento de Organización y Métodos	Jefe de Organización y Métodos	Director de Gestión y Control Interno	Subdirector de Servicios Críticos	Director de Informática y Estadística	Director Ejecutivo

Anexo 2. Boleta de autorización para enrolamiento sin huella dactilar o amputación

RENAP	DIRECCION DE INFORMATICA Y ESTADISTICA - RENAP - BOLETA DE AUTORIZACIÓN PARA ENROLAMIENTO SIN HUELLA DACTILAR O AMPUTACIÓN	RENAP Registro Nacional de las Personas
FO-DI-45		
Edición: 00-00-0000		

Imprimir a doble cara

No. 0-0-0000

Fecha:	**CUI:**	**Código empleado:**	**Oficina Registral No.**
Nombre completo:			
Dependencia a la que pertenece (direción y departamento):			**Departamento y municipio:**
Puesto:			**Fecha inicial de labores en esta oficina registral:**
Motivo de solicitud:	**Fecha inicio:**	**Fecha fin:**	**Indefinido:** ☐ / **Extensión a la que se le puede localizar:**

Al trabajador de RENAP se le hace entrega del usuario y contraseña de red para la conexión al dominio central denominado RENAP.LOCAL, habilitación de VPN, acceso al aplicativo de Consulta de DPI y/o usuario de SIRECI, por lo tanto es el único responsable del uso que le dé. Cualquier anomalía causada por el mal uso o divulgación, se suspenderá indefinidamente de la red, se le deducirán responsabilidades previstas en los documentos normativos vigentes a la fecha del hecho, así como la responsabilidad civil y/o penal que del mismo se derive.

CREAR*	MODIFICAR**	PERFIL EN SIRECI

*Asignación de contraseña a usuario nuevo.
**Cambio de contraseña

Firma y nombre del usuario	Autorizado por jefe inmediato o Registrador Civil de las Personas (firma, nombre y sello)	Autorizado director de área (firma, nombre y sello)

TERMINOS Y CONDICIONES

El presente documento hace de su conocimiento sobre la responsabilidad adquirida por el usuario y contraseña para la autorización de huellas desgastadas o la falta de algún miembro, por lo tanto los siguientes términos y condiciones deben de ser leídos y aceptados.

1. La cuenta de acceso y la contraseña es de uso personal e instranferible. La responsabilidad contraída por el usuario inicia desde la primera validación de huellas desgastadas o la falta de algún miembro.
2. Si en algún momento se detecta que el usuario violó la seguridad de la información se procederá a tomar medidas disciplinarias de conformidad con el Reglamento Interior de Trabajo del Registro Nacional de las Personas -RENAP-. El Departamento de Seguridad Informática deberá deshabilitar inmediatamente el usuario de la red central del Registro Nacional de las Personas -RENAP-.
3. El usuario no deberá por ningún motivo realizar actividades encaminadas a violar la integridad de la información almacenada, siendo el Registrador Civil de las Personas que está dando la fe pública de lo que se registrará.
4. El usuario deberá notificar en forma inmediata a la Dirección de Informática y Estadística si detecta el uso indebido o no autorizado de su cuenta por terceras personas.
5. El usuario está sujeto a auditorías en cualquier momento y sin previo aviso que realice la Dirección de Informática y Estadística.
6. El usuario es el único responsable del uso que se le de a éste, ante cualquier anomalía causada por el mal uso y/o divulgación de la información, se suspenderá al usuario indefinidamente de la red y se enviará copia de la sanción a la Subdirección de Recursos Humanos para que se proceda según Reglamento Interior de Trabajo del Registro Nacional de las Personas -RENAP-.
7. El usuario que firma el presente documento es responsable del usuario y contraseña que se le proporciona para su conexión y se deducirán por la vía correspondiente las responsabilidades civiles y/o penales que del mal uso o divulgación se deriven.
8. Para poder proporcionar el usuario y accesos, se debe adjuntar a esta solicitud copia de nombramiento de la persona, por parte de la Subdirección de Recursos Humanos.

El usuario declara haber leído y aceptado íntegramente los términos y condiciones.

Nombre completo: Firma:_____

Área exclusiva informática y estadística					
Acceso	Día:	Mes:	Año:	Hora:	Operado por:

Página 1 de 1

Elaborado por:	Revisado por:	Revisado por:	Validado por:	Validado por:	Aprobado por:
Departamento de Organización y Métodos	Jefe de Organización y Métodos	Director de Gestión y Control Interno	Subdirector de Servicios Críticos	Director de Informática y Estadística	Director Ejecutivo

Anexo 3. Firma para creación o cambio de autoridad de Registrador Civil de las Personas en el Sistema de Registro Civil -SIRECI-

RENAP	DIRECCIÓN DE INFORMÁTICA Y ESTADÍSTICA DEPARTAMENTO DE SEGURIDAD INFORMÁTICA	Correlativo No. FCCA-___-20__
FO-DIE-SSC-DSI-03	FIRMA PARA CREACIÓN O CAMBIO DE AUTORIDAD DE REGISTRADOR CIVIL DE LAS PERSONAS EN EL SISTEMA DE REGISTRO CIVIL -SIRECI-	

Nombre completo del trabajador:
CUI:

Elaborado por:	Revisado por:	Revisado por:	Validado por:	Validado por:	Aprobado por:
Departamento de Organización y Métodos	Jefe de Organización y Métodos	Director de Gestión y Control Interno	Subdirector de Servicios Críticos	Director de Informática y Estadística	Director Ejecutivo

Anexo 4. Boleta de baja definitiva del usuario de los sistemas

RENAP	DIRECCION DE INFORMATICA Y ESTADISTICA - RENAP - BOLETA DE BAJA DEFINITIVA DEL USUARIO DE LOS SISTEMAS	RENAP Registro Nacional de las Personas
FO-DI-05		
Edición: 00-00-2021		

Imprimir a doble cara

No. 0-0-0000

Red	SIRECI	Correo Electrónico	Consulta DPI

Fecha:	**CUI:**	**Código Empleado:**	**Oficina Registral No.**
Nombre Completo:			
Unidad Administrativa y Departamento al que pertenece:		**Departamento y Municipio:**	
Puesto:		**Fecha de Retiro:**	
Motivo de Retiro de la Institución:			

USUARIO

ACCESOS	Baja	Fecha y Hora Día	Mes	Año	Hora	Persona Encargada
USUARIO DE RED						
CORREO ELECTRÓNICO						
SIRECI, INVENTARIO DPI, VERIFICACION DPI O LOGIN DATOS PERSONALES						
CONSULTA DE DPI						
POINTER						
AUTORIZACIÓN DE ENROLAMIENTO SIN HD O AMPUTACIÓN						
INTRANET						
LIBRO VIRTUAL						
GOBIERNO ELECTRÓNICO						
LIBRO VIRTUAL WEB						
DVIAS Verificación y consulta						

- Todo usuario que deje de laborar en la institución y cuenta con usuarios dentro de la Red del Registro Nacional de las Personas, deberá de contar con una boleta de baja en conjunto con el oficio de baja del puesto.
- Al momento de proceder a dar de baja de la institución a una persona, es responsabilidad de la Subdirección de Recursos Humanos la inactivación del usuario, al momento de causar baja de institución o del puesto.
- La Subdirección de Recursos Humanos deberá llenar el encabezado de la boleta así como la colocación del usuario, las parte correspondiente a accesos deberá ser responsabilidad de la Jefatura de Seguridad Informática.
- La Subdirección de Recursos es la encargada de dar de inactivar a los usuarios de red en el Sistema de Control de Usuarios en Directorio.

Página 1 de 1

Elaborado por:	Revisado por:	Revisado por:	Validado por:	Validado por:	Aprobado por:
Departamento de Organización y Métodos	Jefe de Organización y Métodos	Director de Gestión y Control Interno	Subdirector de Servicios Críticos	Director de Informática y Estadística	Director Ejecutivo

Anexo 5. Autorización de medios extraíbles

RENAP	DEPARTAMENTO DE SEGURIDAD INFORMÁTICA	FO-DIE-SI-01
Dirección de Informática y Estadística	Autorización de medios extraíbles	Versión 01

Solicitud No. _____

Fecha:	CUI:	Usuario:	Dirección:	Departamento:

Nombre completo:	Puesto nominal:	Oficina del RENAP No.

Dispositivo:		Permiso requerido:	No. Serie:
Memoria USB ☐	Disco Duro ☐	☐ Usuario	
Memoria SD ☐	Cámara ☐	☐ Dispositivo	
Puertos USB ☐	Otros: ☐	☐ Director	Dirección IP del equipo:
Especifique: _____			

TÉRMINOS Y CONDICIONES

•El trabajador deberá verificar que este formulario sea firmado por la maxima autoridad de la dependencia a la que pertenece y jefe inmediato.
•El usuario solicitante es el único responsable del uso que se le dé, cualquier anomalía causada por el mal uso o divulgación se suspenderá el privilegio y se le deducirán responsabilidades previstas en los documentos normativos vigentes a la fecha del hecho, así como, la responsabilidad civil y/o penal que del mismo se derive.
• El usuario es el responsable de los dispositivos y medios que le hayan sido asignados, por lo que, deberá asegurar el resguardo de la información contenida en los mismos.
• El usuario deberá revisar la presencia de virus en el dispositivo asignado cuando éste sea utilizado fuera de la red del RENAP.
• El usuario deberá dar buen uso a los medios removibles asignados.
• Solo el usuario registrado puede reportar los incidentes del dispositivo a su cargo.
• Este formulario "Autorización de medios extraíbles" deberá entregarse mediante oficio a la Dirección de Informática y Estadística indicando el motivo por el que se solicita el permiso requerido.
• En caso de extravió del dispositivo, el usuario a su cargo deberá informar a la Dirección de Informática y Estadística para retirar los permisos al mismo.

Usuario solicitante (firma, nombre)	Autorizado por jefe inmediato (firma, nombre, sello)	Aprobado por director de área (firma, nombre, sello)

Área exclusiva Direccion de Informática y Estadística :				
Día:	Mes:	Año:	Hora:	Operado por:

Elaborado por:	Revisado por:	Revisado por:	Validado por:	Validado por:	Aprobado por:
Departamento de Organización y Métodos	Jefe de Organización y Métodos	Director de Gestión y Control Interno	Subdirector de Servicios Críticos	Director de Informática y Estadística	Director Ejecutivo

Anexo 6. Boleta de acceso políticas de "Firewall"

RENAP	DIRECCION DE INFORMATICA Y ESTADISTICA -RENAP-	RENAP Registro Nacional de las Personas
FO-DI-41	BOLETA DE ACCESO POLÍTICAS DE FIREWALL	
Edición: 01 01/2021		

No. _____

Llenar todos los campos con letra clara y de molde

IMPRIMIR A DOBLE CARA

Fecha en que solicita el acceso:	**No. CUI:**	
Nombre Completo:		
Puesto		
Nombre de la Oficina Registral o Dirección/Unidad Administrativa:	**Correo Electrónico Institucional:**	
IP Origen:	**IP Destino:**	**Puerto Destino (Aplicación si es el caso):**
Tipo de Acceso: (Marcar solo una opción) Temporal ☐ Indefinido ☐	**Fecha Inicial del acceso:**	**Fecha final del Acceso (Si es Acceso Temporal):**
Indique el horario en que deberá estar habilitada la conexión (si aplica):		
Indique la causa o motivo por el cual solicita realizar la conexión:		
Descripción de la actividad a realizar:		

Al trabajador del RENAP se autoriza la conexión solicitada, por lo tanto, es el único responsable del uso que le dé a esta conexión. Cualquier anomalía causada por el mal uso de esta conexión, se suspenderá la misma indefinidamente según sea el caso y se enviará copia de la sanción a la Sub-Dirección de Recursos Humanos para que se proceda según Reglamento Interior de Trabajo del Registro Nacional de las Personas -RENAP. Además, se deducirán por la vía correspondiente la responsabilidad civil y/o penal que del mal uso o divulgación se deriven.

Firma del Usuario Solicitante	*Autorización de Acceso Jefe Inmediato (firma, nombre y sello)*	*Autorización de Operación de Acceso Jefe de Seguridad Informática (firma, nombre y sello)*	*Vo.Bo. Director de Informática y Estadística (firma, nombre y sello)*

Elaborado por:	Revisado por:	Revisado por:	Validado por:	Validado por:	Aprobado por:
Departamento de Organización y Métodos	Jefe de Organización y Métodos	Director de Gestión y Control Interno	Subdirector de Servicios Críticos	Director de Informática y Estadística	Director Ejecutivo

RENAP FO-DI-41 Edición: 01 01/2021	**DIRECCION DE INFORMATICA Y ESTADISTICA -RENAP-** **BOLETA DE ACCESO** **POLÍTICAS DE FIREWALL**	RENAP Registro Nacional de las Personas

TÉRMINOS Y CONDICIONES

En el acceso del usuario a la red del RENAP

El presente documento hace de su conocimiento sobre la responsabilidad adquirida por el usuario al momento de acceder a la conexión autorizada, especificada en el formulario. Por lo tanto, los siguientes términos y condiciones deben de ser leídos y aceptados.

1. La conexión se efectuará EXCLUSIVAMENTE desde el origen hasta el destino según el puerto o aplicación solicitada.
2. El usuario utilizará la conexión configurada EXCLUSIVAMENTE para el motivo por el cual lo indica en este formulario, y es responsable EXCLUSIVO del uso que se le dé a tal conexión.
3. El usuario deberá en forma inmediata notificar al Departamento de Seguridad Informática de la Dirección de Informática y Estadística si detecta el uso indebido o no autorizado de la conexión. El Departamento de Seguridad Informática realizará las acciones inmediatas correspondientes en cuanto al usuario de la red o la conexión solicitada según sea el caso.
4. La conexión a través de firewall está sujeto a auditorias en cualquier momento y sin previo aviso por parte del Departamento de Seguridad Informática de la Dirección de Informática y Estadística.
5. El usuario o solicitante no deberá por ningún motivo realizar actividades encaminadas a violar la seguridad de los servicios y sistemas utilizados en el RENAP a través de la conexión solicitada.
6. El usuario o solicitante deberá reportar cualquier problema referente a la conexión solicitada al Departamento de Seguridad Informática.

El Usuario declara haber leído y aceptado íntegramente los términos y condiciones.

Nombre Completo: _____ Firma: _____

Area exclusiva del Depto. De Seguridad Informática

Operado por: _____

Día	Mes	Año	Hora

Observaciones:

_____

_____

Elaborado por:	Revisado por:	Revisado por:	Validado por:	Validado por:	Aprobado por:
Departamento de Organización y Métodos	Jefe de Organización y Métodos	Director de Gestión y Control Interno	Subdirector de Servicios Críticos	Director de Informática y Estadística	Director Ejecutivo

Control de cambios

Versión	Fecha	No. de folios	Unidades involucradas	Descripción
03	2022	68	Dirección de Informática y Estadística	Manual de Normas y Procedimientos de Departamento de Seguridad Informática
02	2021	68	Dirección de Informática y Estadística	Manual de Normas y Procedimientos de Departamento de Seguridad Informática, aprobado por medio de Acuerdo de Dirección Ejecutiva número DE-608-2021.
01	2020	64	Dirección de Informática y Estadística	Manual de Normas y Procedimientos de Departamento de Seguridad Informática, aprobado por medio de Acuerdo de Dirección Ejecutiva número DE-595-2020.