1. OBJETIVO

Implementar acciones de seguridad de la información y seguridad informática digital en la Registraduría Nacional del Estado Civil (RNEC) mediante la gestión de vulnerabilidades, incidentes, activos de seguridad, retiro de equipos, acceso a VPN e ingreso a áreas restringidas de infraestructura tecnológica, con el fin de mantener la integridad, disponibilidad y confidencialidad de la información de la Entidad.

2. ALCANCE

Se inicia con gestión de activos de seguridad, continúa con la gestión de vulnerabilidades, sigue con la gestión de incidentes, gestión de solicitudes de retiro de equipos, servicio de acceso a VPN, y finaliza con la solicitud de ingreso a áreas restringidas de infraestructura tecnológica. Este procedimiento es aplicable a todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Registraduría Nacional del Estado Civil.

3. ÁMBITO DE APLICACIÓN

Todos los procesos y procedimientos se aplican al nivel central, desconcentrado, fondos adscritos, contratistas y terceros.

4. BASE DOCUMENTAL

- Documento de análisis de vulnerabilidades (aliado tecnológico)
- Formato “Matriz de inventario, clasificación y valoración de activos de información” (GIFT09)
- Formato “Autorización salida de equipos” (STFT10)
- Formato “Bitácora de acceso a áreas restringidas de infraestructura tecnológica” (GITF02)
- Formato “Formato único para solicitud de acceso remoto seguro a sistemas de información a través de VPN C2S TIPO SSL” (GIFT03)
- Matriz de Seguimiento de Incidentes
- Matriz de Seguimiento de Incidentes
- Manual de Instalación y configuración del agente vpn ztna para consulados (GIMN02)
- Manual de instalación y configuración del agente vpn ztna para RNEC (GIMN03)

Formato aprobado: 09/08/2019 - versión n. º 1

- Instructivo de instalación y configuración del agente vpn ztna para notarias (GIIN01)
- Instructivo de instalación y configuración del agente vpn ztna para clínicas y hospitales (GIIN02)

5. BASE LEGAL

Norma (número y fecha)	Directriz legal
Constitución Política de Colombia de 1191, artículo 209.	La función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad.
Ley 190 de 1995, Estatuto Anticorrupción	Por la cual se dictan normas tendientes a preservar la moralidad en la Administración Pública y se fijan disposiciones con el fin de erradicar la corrupción administrativa.
Ley 962 del 2005. Por el cual por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.	Dicta disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
Ley 1341 de 2009 – "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC-, se crea la agencia nacional de espectro y se dictan otras disposiciones."	Determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información.
Ley 1672 de 2013. Por la cual se establecen los lineamientos para la adopción de una política pública de gestión integral de residuos de aparatos eléctricos y electrónicos (raee), y se dictan otras disposiciones	La presente ley tiene por objeto establecer los lineamientos para la política pública de gestión integral de los Residuos de Aparatos Eléctricos y Electrónicos (RAEE) generados en el territorio nacional. Los RAEE son residuos de manejo diferenciado que deben gestionarse de acuerdo con las directrices que para el efecto establezca el Ministerio de Ambiente y Desarrollo Sostenible.
Ley 2088 de 2021. Por la cual se regula el trabajo en casa y se dictan otras disposiciones	Tiene por objeto regular la habilitación de trabajo en casa como una forma de prestación del servicio en situaciones ocasionales, excepcionales o especiales, que se presenten en el marco de una relación laboral, legal y reglamentaria con el Estado o con el sector privado, sin que conlleve variación de las condiciones

Norma (número y fecha)	Directriz legal
	laborales establecidas o pactadas al inicio de la relación laboral.
Decreto 2573 de 2014. Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea.	Define los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y participativo y que preste mejores servicios con la colaboración de toda la sociedad.
Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.	Compila normatividad referente al sector de tecnologías de la información y las comunicaciones. Su capítulo 6 contiene las disposiciones sobre el tratamiento de datos personales, seguridad y privacidad de la información.
Decreto 1010 de 2000. Artículo 41. Gerencia de Informática.	Funciones de la Gerencia de Informática.
Resolución 4173 de 2016. por la cual se derogan las resoluciones 13829 de diciembre 12 de 2011 y 9025 de octubre 30 de 2012, generando nuevas Políticas de Seguridad de la Información.	Define las Políticas de Seguridad de la Información de la Registraduría Nacional del Estado Civil, con el fin de regular la Gestión de la seguridad de la información al interior de la entidad.
Resolución 4154 de 2016. por la cual se establecen funciones del comité de seguridad informática de la Registraduría Nacional del Estado Civil.	Modifica la Resolución 13860 de 2016, que conforma el comité de seguridad de la información de la Registraduría Nacional del Estado Civil, y estableciendo sus funciones.
Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.	Establece los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital.
Resolución 746 de 2022. Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución número 500 de 2021.	Adiciona y complementa la resolución 500 de 2021, además en su anexo # 2, se encuentra la relación con proveedores de seguridad digital.
Norma ISO-IEC 27000	Conjunto de estándares creados y gestionados por la *Organización Internacional para la Estandarización* (ISO) y *la Comisión Electrónica Internacional* (IEC). Ambas organizaciones internacionales están participadas por multitud de países, lo que garantiza su amplia difusión, implantación y reconocimiento en todo el mundo.

Norma (número y fecha)	Directriz legal
Norma Técnica Colombiana NTC-ISO-IEC 27001 (Primera actualización, traducción 2013-12-20)	La NTC ISO 27001 es una norma colombiana que hace posible que las organizaciones aseguren la confidencialidad y al mismo tiempo la integridad de toda la información que tengan. La versión internacional de la norma que está vigente es la ISO 27001:2013
Resolución 3308 del 11 de abril de 2024. Por la cual se adopta la política de Seguridad de la Información de la Registraduría Nacional del Estado Civil y se dictan otras disposiciones.	Define la adopción de las Políticas de Seguridad de la Información de la Registraduría Nacional del Estado Civil.

6. DEFINICIONES

Fuente: ISO/IEC 27000:2018, ISO/IEC 27040:2015, ISACA Fundamentals, Ley 2088 de 2021 y otros.

Activo: Recurso de valor tangible o intangible que debería ser protegido, lo que comprende personas, información, infraestructura, finanzas y reputación.
Aplicación: Programa informático diseñado como una herramienta para realizar operaciones o funciones específicas.
Autenticidad: Propiedad que consiste en que una entidad es lo que afirma ser.
Código malicioso: Es un tipo de código informático dañino, diseñado para vulnerar o crear vulnerabilidades en un sistema informático.
Confiabilidad: Uniformidad en cuanto al comportamiento y los resultados deseados.
Confidencialidad: Propiedad según la cual la información no está disponible para personas, entidades, procesos o sistemas no autorizados, ni se da a conocer a personas, entidades, procesos o sistemas no autorizados.
Continuidad del negocio: Recopilación documentada de los procedimientos y la información que se preparan para su uso en caso de incidente grave, con el objetivo de poder continuar prestando sus servicios críticos en un nivel aceptable predefinido.
Control de acceso: Medio para asegurar que el acceso a los activos esté autorizado y restringido en función de requisitos relacionados con la actividad y la seguridad.
Criptografía: Es una técnica utilizada para salvaguardar los datos e impedir que terceros no autorizados puedan acceder a información valiosa o alterarla para su propio beneficio o en perjuicio de otros.
Data center: Es un centro de procesamiento de datos, localizado en una construcción de gran tamaño donde se albergan los equipos electrónicos

necesarios para mantener un sistema informático y sistemas de información.
Disponibilidad: Cualidad de accesible y utilizable a demanda por parte de una entidad autorizada.
Dispositivo móvil: Son dispositivos de comunicación portátiles que se pueden utilizar para comunicaciones de voz y de datos, como los teléfonos móviles, portátiles, tabletas, entre otros.
Hardware: Componentes físicos tangibles, de un sistema informático, como los componentes eléctricos, electrónicos, electromecánicos y mecánicos.
Incidente de seguridad de la información: Compromiso que, de manera accidental o ilegal, da lugar a la destrucción, la pérdida, la alteración, la divulgación, o el acceso no autorizado a datos transmitidos, almacenados o procesados de otra manera.
Infraestructura de TI: Son todos aquellos elementos tecnológicos de hardware y software; servidores, computadores, portátiles, impresoras, switch, router, equipos de seguridad informática, escáner, cableado estructurado, equipos de comunicaciones e internet, red LAN y WAN que hacen parte de la Entidad.
Integridad: Cualidad de exacto y completo.
Medios removibles: Dispositivo de almacenamiento de información que sea extraíble de su gestor de información, como unidades USB, discos duros portables, tarjetas SD, CD, DVD, unidades de cinta, entre otros.
Nube: Es una red de recursos informáticos que provee un servicio de computación que procesa y almacena datos por medio de una red.
Nube privada: Es un modelo de implementación de nube en el que los recursos informáticos son de propiedad reservada, en la cual una organización aloja y gestiona su sistema informático.
Nube pública: Es un tipo de computación en la nube en el que un proveedor de servicios en la nube facilita recursos informáticos a través de Internet público, en la cual una organización aloja y gestiona su sistema informático.
Proveedor: Entidad encargada de abastecer un servicio o producto necesario para que desarrolle su actividad principal.
Red: Es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos, también conocida como Red de comunicaciones.
Seguridad de la información: Son medidas preventivas que toma la Organización para resguardar la información que está automatizada, tomando como base fundamental pilares de seguridad como; integridad, disponibilidad, confidencialidad, autenticidad, responsabilidad, aceptabilidad, confiabilidad y no repudio.
Sistema de información: Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información, que incluye el entorno operativo.
Sistema informático: Sistema que permite almacenar y procesar información, con un conjunto de partes interrelacionadas de hardware, software y personal informático.
Software: Parte lógica e intangible que poseen los sistemas informáticos
Teletrabajo: Permite trabajar en un lugar diferente a la oficina, el cual se realiza en un lugar diferente de las sedes físicas de la Entidad, mediante la utilización de las nuevas tecnologías de la comunicación.

Trabajo en casa: Es una opción que tiene el trabajador para desarrollar sus funciones sin cambiar sus actividades ni sus condiciones, que aplica para circunstancias ocasionales y excepcionales.
Vulnerabilidad: Debilidad, susceptibilidad o defecto de un activo o control que pueden ser explotados por una o más amenazas

7. POLÍTICAS DE OPERACIÓN

- Para el tratamiento de la seguridad de la información de la Entidad, se tendrá como política lo estipulado en la resolución 3308 de abril 11 de 2024. Políticas de Seguridad de la Información.

8. DESCRIPCIÓN DEL PROCEDIMIENTO

#	ACTIVIDAD	TIEMPO	RESPONSABLE	PUNTO DE CONTROL	REGISTROS Y/O DOCUMENTOS
1	**Levantar el inventario de los activos de seguridad.** El funcionario Designado de la Coordinación de Administración de Infraestructura junto con los propietarios de los activos o el personal asignado de cada dependencia de la Entidad, diligencian el formato GIFT09 Matriz de inventario, clasificación y valoración de activos de información.	Anualmente	Funcionarios designados por la Coordinación de Administración e Infraestructura Tecnológica y Propietarios de los activos	Reuniones con los propietarios y custodios de los activos de información	Actas de Reunión y formato GIFT09 Matriz de inventario, clasificación y valoración de activos de información
2	**Clasificar y valorar los activos de Seguridad.** El funcionario Designado de la Coordinación de Administración de Infraestructura junto con los propietarios de los activos o el personal asignado de cada dependencia de la Entidad, clasifican y valoran los activos según lo establecido en el formato GIFT 09 Matriz de inventario, clasificación y valoración de activos de información.	Anualmente	Funcionarios designados por la Coordinación de Administración e Infraestructura Tecnológica y Propietarios de los activos	Reuniones con los propietarios y custodios de los activos de información	Actas de Reunión y formato GIFT09 Matriz de inventario, clasificación y valoración de activos de información
3	**Actualizar los Activos de Seguridad.**	Anualmente	Funcionarios designados por la Coordinación de Administración	Reuniones con los propietarios y	Matriz de inventario, clasificación y

#	ACTIVIDAD	TIEMPO	RESPONSABLE	PUNTO DE CONTROL	REGISTROS Y/O DOCUMENTOS
	El funcionario Designado de la Coordinación de Administración de Infraestructura junto con los propietarios de los activos o el personal asignado de cada dependencia de la Entidad actualizan en la matriz de inventario, clasificación y valoración de activos de información. En la cual se modifica, crea o elimina los activos de seguridad.		e Infraestructura Tecnológica y Propietarios de los activos	custodios de los activos de información	valoración de activos de información (GIFT09)
4	**Analizar y clasificar los riesgos de la matriz de los activos de Seguridad.** El funcionario Designado de la Coordinación de Administración de Infraestructura junto con los propietarios de los activos o el personal asignado de cada dependencia de la Entidad, analizan y clasifican los riesgos de la matriz de activos según los que tengan mayor probabilidad de ocurrencia.	Anualmente	Funcionarios designados por la Coordinación de Administración e Infraestructura Tecnológica y Propietarios de los activos	Reuniones con los propietarios y custodios de los activos de información	Matriz de inventario, clasificación y valoración de activos de información (GIFT09)
5	**Detectar las vulnerabilidades.** Una vez clasificados los riesgos de la matriz de inventario, clasificación y valoración de activos de información y el escaneo de vulnerabilidades realizado por las herramientas del aliado tecnológico se detectan las brechas y se clasifican según el impacto.	Mensualmente	Funcionarios designados por la Coordinación de Administración e Infraestructura Tecnológica y Aliado Tecnológico	Herramienta se Seguimiento	Documento de análisis de vulnerabilidades (aliado tecnológico)
6	**¿Se ha detectado alguna vulnerabilidad?** **SÍ:** Ir a la actividad 7 **NO**: Ir a la actividad 5				
7	**Gestionar las Vulnerabilidades.** Se realiza un análisis de vulnerabilidades sobre la infraestructura tecnológica.	Mensualmente	Funcionarios designados por la Coordinación de Administración e Infraestructura Tecnológica	Reuniones periódicas para revisión y actualización de documentos	Documento de análisis de vulnerabilidades (aliado tecnológico)
8	**Definir plan de acción.**	Mensualmente	Funcionarios designados por la Coordinación de Administración	Cronograma y plan de trabajo	Plan de acción

Formato aprobado: 09/08/2019 - versión n. º 1

#	ACTIVIDAD	TIEMPO	RESPONSABLE	PUNTO DE CONTROL	REGISTROS Y/O DOCUMENTOS
	Planear las actividades concernientes para mitigar las vulnerabilidades encontradas y se socializa para aprobación.		e Infraestructura Tecnológica		
9	**Ejecutar el plan de acción** Se ejecuta el plan de acción y se analiza su efectividad en la mitigación de las vulnerabilidades.	Mensualmente	Funcionarios designados por la Coordinación de Administración e Infraestructura Tecnológica	Reuniones periódicas para revisión y actualización de documentos	Informe de ejecución.
10	**¿Se mitigaron las vulnerabilidades?** **Sí:** Continúe con la actividad 11 **No:** Continúe a la actividad 7				
11	**¿Se ha detectado algún incidente de seguridad?** **SI:** Continúe con la actividad 12 **NO:** Continúe con la actividad 18				
12	**Gestionar los Incidentes de Seguridad y Notificar el evento.** Los usuarios o administradores notifican el evento detectado por medio de: alertas de las plataformas, caídas del sistema, reportes, registros de herramientas administrativas, entre otros.	Cuando se presente el evento	Funcionarios designados por la Coordinación de Administración e Infraestructura Tecnológica	Medio por el que se detecta el posible incidente	Matriz de Seguimiento de Incidentes
13	**Analizar el evento.** Se analiza el evento y material complementario tal como logs, archivos, código malicioso u otros artefactos.	Cuando se presente el evento	Funcionarios designados por la Coordinación de Administración e Infraestructura Tecnológica	Reuniones para revisión	Matriz de Seguimiento de Incidentes
14	**Registrar el incidente.**	Cuando se presente el	Funcionarios designados por la Coordinación de Administración	Registro en la matriz	Matriz de Seguimiento de

#	ACTIVIDAD	TIEMPO	RESPONSABLE	PUNTO DE CONTROL	REGISTROS Y/O DOCUMENTOS
	Todo incidente y/o evento de seguridad de la información deberá ser registrado en la "Matriz de Seguimiento de Incidentes", documentando los datos solicitados en el mismo incluyendo la clasificación del incidente según su criticidad	evento	e Infraestructura Tecnológica		Incidentes
15	**Generar plan de acción.** Se genera un plan de acción que permita definir las actividades que se deben ejecutar para la gestión del Incidente de Seguridad. Para ello, deberá determinar los lugares a intervenir frente al recaudo de las evidencias, las acciones de contención, erradicación y recuperación frente a los servicios y/o plataformas afectadas por el incidente.	Cuando se presente el evento	Funcionarios designados por la Coordinación de Administración e Infraestructura Tecnológica	Reuniones para revisión	Plan de acción
16	**Verificar la situación actual del incidente.** Se verifica la situación actual del incidente (ya terminó, está en proceso, ya se tiene bajo control), obteniendo mayor cantidad de información del incidente, complementando el Registro de Incidentes.	Cuando se presente el evento	Funcionarios designados por la Coordinación de Administración e Infraestructura Tecnológica	Reuniones para revisión	Matriz de Seguimiento de Incidentes
17	**¿Se controló el incidente de seguridad?** **SÍ:** continúa con la actividad Fin **NO**: ir a la actividad 12				
18	**¿Se requiere el retiro de un equipo de Sede CAN?** **SI:** Continúe con la actividad 19 **NO:** Continúe con la actividad 22				
19	**Diligenciar Formato autorización salida de equipos (STFT10) sede CAN.** El funcionario que va a retirar el equipo debe diligenciar el formato para la salida del equipo.	Cuando se requiera	Funcionario que retira el equipo	Revisión funcionario que autoriza	Formato autorización salida de equipos (STFT10)

Formato aprobado: 09/08/2019 - versión n. º 1

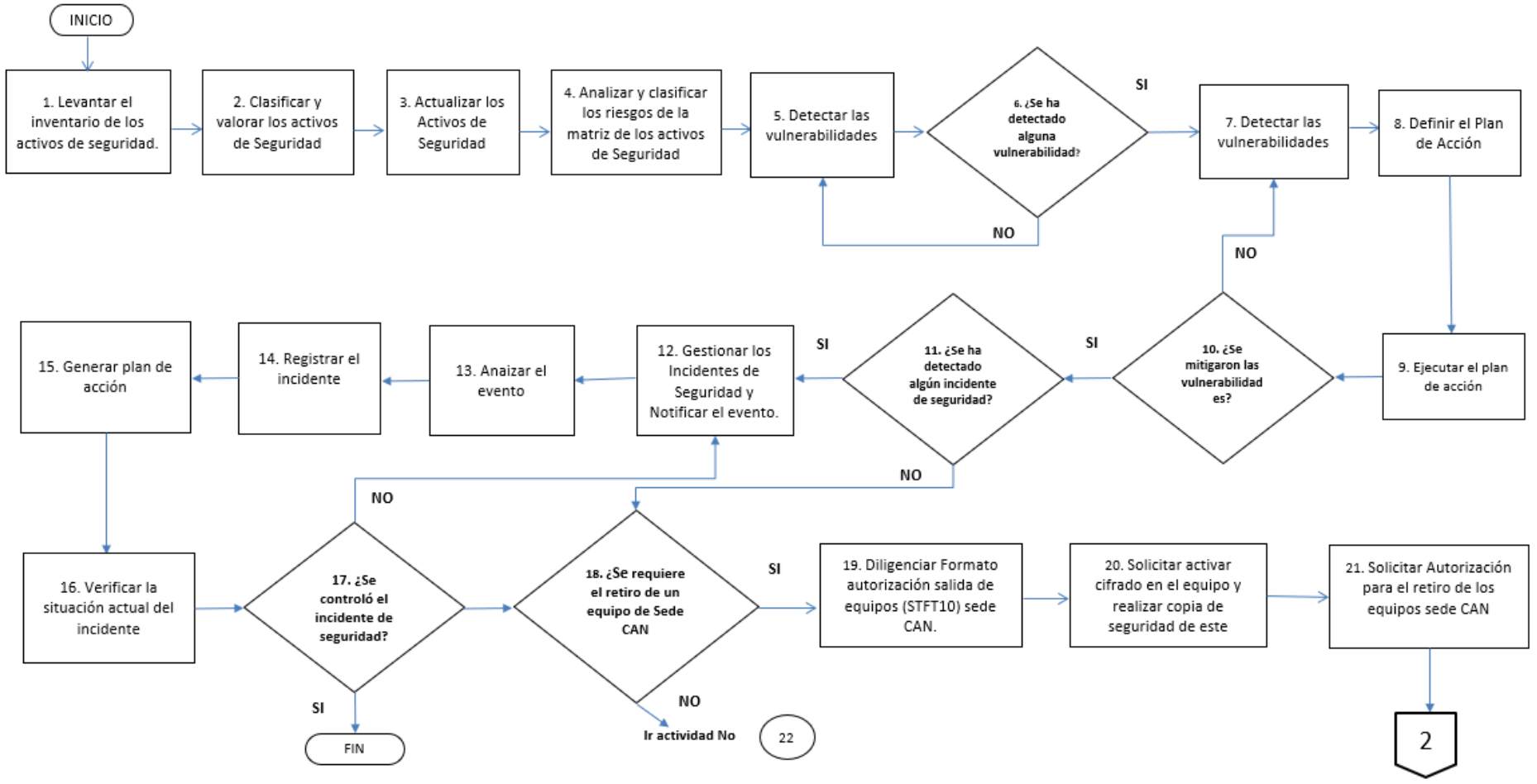
#	ACTIVIDAD	TIEMPO	RESPONSABLE	PUNTO DE CONTROL	REGISTROS Y/O DOCUMENTOS
20	**Solicitar activar cifrado en el equipo y realizar copia de seguridad de este.** El funcionario que va a retirar el equipo debe solicitar que se realice copia de seguridad y la ejecución de cifrado en el equipo, En caso de no aplicar el cifrado se debe justificar el motivo por el cual no se aplica.	Cuando se requiera	Funcionarios designados por la Coordinación de soporte técnico y telecomunicaciones	Revisión funcionario que autoriza	Formato autorización salida de equipos (STFT10)
21	**Solicitar Autorización para el retiro de los equipos sede CAN** Se procede a firmar el formato por parte de quien autoriza el retiro de los equipos.	Cuando se requiera	Coord. Soporte técnico y telecomunicaciones	Revisión funcionario que autoriza	Formato autorización salida de equipos (STFT10)
22	**¿Se requiere acceso seguro a sistemas de información a través de VPN tipo SSL?** **SI:** Continúe con la actividad 23 **NO:** Continúe con la actividad 26				
23	**Solicitar el Servicio de Acceso a VPN .** El usuario allegara el requerimiento de acceso seguro a sistemas de información a través de la VPN, mediante el formato “Solicitud de acceso remoto seguro a sistemas de información a través de VPN C2S tipo SSL” - GIFT03 por medio físico a la Gerencia de Informática o al correo electrónico designado.	1 hora	Usuario	Solicitud de acceso	Formato único para solicitud de acceso remoto seguro a sistemas de información a través de VPN C2S TIPO SSL (GIFT03)
24	**Autorizar Requerimiento.** Evaluar el requerimiento de acceso seguro a sistemas de información a través de VPN tipo SSL, previamente avalado por la coordinación de Protección de Datos personales y/o el responsable del sistema de información al cual se va a	3 días	Funcionarios designados por la Coordinación de Administración e Infraestructura Tecnológica	Documento Diagnostico	Documento Diagnóstico

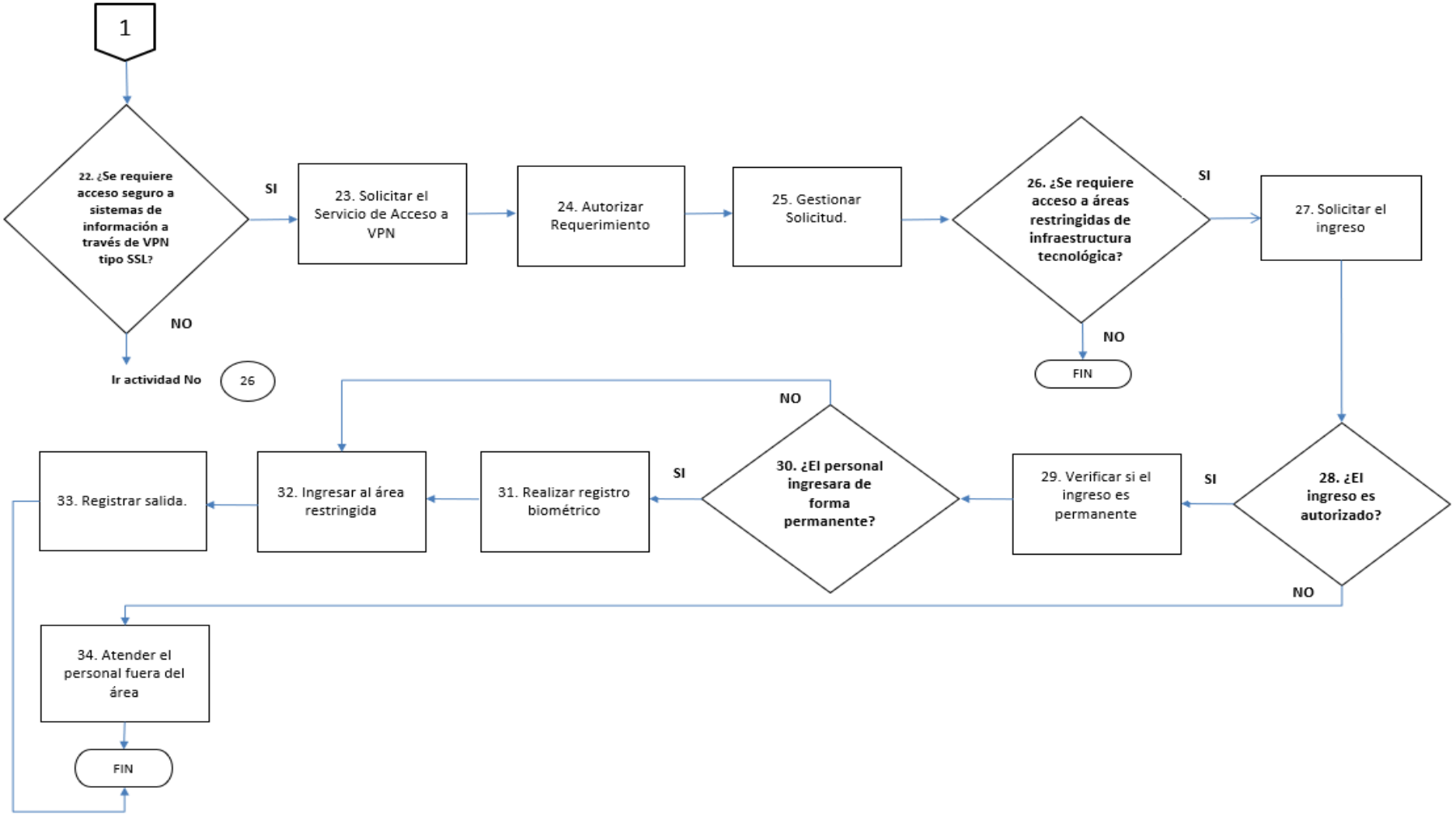
Formato aprobado: 09/08/2019 - versión n. º 1

#	ACTIVIDAD	TIEMPO	RESPONSABLE	PUNTO DE CONTROL	REGISTROS Y/O DOCUMENTOS
	acceder.				
25	**Gestionar Solicitud.** Enviar correo electrónico al encargado de la administración del Appliance de VPN, la solicitud de acceso seguro a sistemas de información a través de VPN tipo SSL.	1 día	Funcionarios designados por la Coordinación de Administración e Infraestructura Tecnológica	Correo electrónico	Correo electrónico
26	**¿Se requiere acceso a áreas restringidas de infraestructura tecnológica?** **SI:** Continúe con la actividad 27 **NO:** Fin del procedimiento				
27	**Solicitar el ingreso.** El usuario realizara la solicitud de acceso mediante correo electrónico al Coordinador de Administración de Infraestructura.	Cuando se requiera	Usuario	Correo electrónico	Correo electrónico.
28	**¿El ingreso es autorizado?** **SI:** ir a la actividad 29. **NO:** ir a la actividad 34				
29	**Verificar si el ingreso es permanente.** Se definirá el personal que tendrá ingreso permanente a las áreas con acceso restringido	Cuando se requiera	Usuario	Correo electrónico	Correo electrónico.
30	**¿El personal ingresara de forma permanente?** **Si:** Pase a la actividad 31 **No:** Pase a la actividad 32				

#	ACTIVIDAD	TIEMPO	RESPONSABLE	PUNTO DE CONTROL	REGISTROS Y/O DOCUMENTOS
31	**Realizar registro biométrico.** Se definirá el personal que tendrá ingreso permanente a las áreas con acceso restringido y se procederá a realizar el registro biométrico respectivo.	cuando se requiera	Funcionarios designados por la Coordinación de Administración e Infraestructura Tecnológica	Herramienta de Registro Biométrico	Registro Biométrico
32	**Ingresar al área restringida.** Si el personal no cuenta con Registro biométrico Una vez autorizado el ingreso, deberá realizarse en compañía del funcionario designado por el coordinador de Infraestructura.	1 día	Funcionarios designados por la Coordinación de Administración e Infraestructura Tecnológica.	Formato Bitácora de acceso GIFT02	Formato Bitácora de acceso (GIFT02)
33	**Registrar salida.** Una vez realizada la visita, se deberá registrar la salida del visitante con hora fecha y firma en el formato GIFT02 *"Bitácora de acceso áreas restringidas".*	1 día	Funcionarios designados por la Coordinación de Administración e Infraestructura Tecnológica.	Formato Bitácora de acceso GIFT02	Formato Bitácora de acceso (GIFT02)
34	**Atender el personal fuera del área.** Si el personal no cuenta con Registro biométrico y el ingreso no es autorizado se la persona se atenderá por parte del funcionario designado por el coordinador de Infraestructura en el área fuera.	cuando se requiera	Funcionarios designados por la Coordinación de Administración e Infraestructura Tecnológica	Correo electrónico	Correo electrónico

9. FLUJOGRAMA




1
22. ¿Se requiere acceso seguro a sistemas de información a través de VPN tipo SSL?
SI
23. Solicitar el Servicio de Acceso a VPN
24. Autorizar Requerimiento
25. Gestionar Solicitud.
26. ¿Se requiere acceso a áreas restringidas de infraestructura tecnológica?
SI
27. Solicitar el ingreso
NO
FIN
NO
Ir actividad No
26
NO
30. ¿El personal ingresara de forma permanente?
SI
31. Realizar registro biométrico
32. Ingresar al área restringida
33. Registrar salida.
29. Verificar si el ingreso es permanente
SI
28. ¿El ingreso es autorizado?
NO
34. Atender el personal fuera del área
FIN

10. ANÁLISIS DE GESTIÓN

Gestionar Activos de Seguridad	Anualmente
Clasificar y valorar los activos de seguridad	Anualmente
Ejecutar análisis de vulnerabilidades sobre Servidores.	Mensualmente
Detectar vulnerabilidades	Mensualmente
Definir plan de acción	Mensualmente
Ejecutar el plan de acción	Mensualmente
Notificación de evento (incidente)	Cuando se presente el evento
Analizar el evento	Cuando se presente el evento
Registrar el incidente	Cuando se presente el evento
Generar plan de acción	Cuando se presente el evento
Verificar la situación actual del incidente	Cuando se presente el evento
Diligenciar solicitud de retiro de equipos organización electoral Sede CAN	Cuando se requiera
Activar cifrado en el equipo	Cuando se requiera
Autorización	Cuando se requiera
Solicitar el servicio de acceso a VPN	1 hora
Autorizar Requerimiento	3 días
Gestionar Solicitud	1 día
Definir el ingreso y realizar registro biométrico a áreas restringidas de infraestructura tecnológica	cuando se requiera
Solicitar el ingreso	Cuando se requiera
Ingresar al área restringida	cuando se requiera
Registrar salida	cuando se requiera

11. ANEXOS

NA

12. CONTROL DE CAMBIOS

ASPECTOS QUE CAMBIARON EL DOCUMENTO DETALLES DE LOS CAMBIOS EFECTUADOS	RESPONSABLE DE LA SOLICITUD DEL CAMBIO	FECHA DEL CAMBIO DD/MM/AAAA	VERSIÓN
Procedimiento nuevo	Gerencia de Informática	30/01/2023	0
Actualización de la base documental con la inclusión del Manual de políticas internas y controles de seguridad de la información.	Gerencia de Informática	27/02/2024	1
Actualización del alcance, de la base legal, la Política de Operación, las actividades, el flujograma y el análisis de gestión.	Gerencia de Informática	18/03/2024	2
Actualización base legal, base documental y en las políticas de operación	Gerencia de Informática	25/06/2024	3
Actualización de la base documental con la inclusión del Manual de instalación y configuración del agente vpn ztna para Consulados y RNEC.	Gerencia de Informática	26/05/2025	4
Actualización de la base documental con la inclusión del Manual de instalación y configuración del agente vpn ztna para Hospitales, clínicas y notarias	Gerencia de Informática	24/06/2025	5

Formato aprobado: 09/08/2019 - versión n. º 1

ELABORÓ:	**REVISÓ**:	**APROBÓ**:
Edwin Jimmy Camargo Avendaño Analista de Sistemas Ruth Maritza Maldonado Rodriguez Profesional Especializado Andres Acosta Blanquiceth Profesional Universitario	Eduardo Emilio Calderón Narváez Coordinador de Administración e Infraestructura Tecnológica Betsy Maria Ospino Plata Coordinadora de Soporte Técnico y Telecomunicaciones Andrea Rosas Tobito Coordinadora Integración y Gestión	Hoslander Adlai Saenz Barrera Gerente de Informática (EF)
	REVISIÓN TÉCNICA: Candelaria Lucía Teherán Fontalvo Profesional Universitario Oficina de Planeación	**APROBACIÓN TÉCNICA**: Zamira Marcela Gomez Carrillo Jefe de la Oficina de Planeación
FECHA: 20/06/2025	**FECHA:** 24/06/2025	**FECHA:** 24/06/2025