	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 1 de 111

MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL – SGSISD

FISCALÍA GENERAL DE LA NACIÓN

2022




	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 2 de 111

TABLA DE CONTENIDO

INTRODUCCIÓN	4
1. OBJETIVO	5
2. ALCANCE	5
3. DEFINICIONES Y SIGLAS	5
4. MARCO LEGAL / DOCUMENTOS DE REFERENCIA	16
4.1. OTROS DOCUMENTOS DE REFERENCIA	17
5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	18
5.1. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA FGN ... 18	
5.2. ALCANCE DE LA POLÍTICA	18
6. MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA FISCALÍA GENERAL DE LA NACIÓN	19
6.1. CICLO DE OPERACIÓN DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	20
6.2. DESARROLLOS DE LAS FASES DEL CICLO DE OPERACIÓN DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA FGN	22
6.3. DESARROLLO DE LOS MOMENTOS DEL CICLO DE OPERACIÓN DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA FGN.	25
6.4. ESQUEMA DEL CICLO DE OPERACIÓN DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MGSÍ DE LA FGN.	27
7. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL (SGSISD)	28
7.1. OBJETIVO	28
7.2. ALCANCE DEL SGSISD	29
7.3. ROLES Y RESPONSABILIDADES	30
8. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y DE SEGURIDAD DIGITAL ..	41
8.1. LINEAMIENTOS DE CUMPLIMIENTO PARA LA SEGURIDAD DE LA INFORMACIÓN EN LOS PROCESOS	43
8.2. SEGURIDAD DE LA INFORMACIÓN PARA LOS RECURSOS HUMANOS	50

 FISCALÍA <small>GENERAL DE LA NACIÓN</small>	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 3 de 111

8.3. SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE TECNOLOGÍAS DE LAS INFORMACIÓN Y LAS COMUNICACIONES	51
8.4. SEGURIDAD DE LA INFORMACIÓN EN LOS ACTIVOS FÍSICOS	61
8.5. MEJORA CONTINUA EN LA SEGURIDAD DE LA INFORMACIÓN	63
8.6. PLANEACIÓN ESTRATÉGICA DE LA SEGURIDAD DE LA INFORMACIÓN ..	64
8.7. SEGURIDAD DE LA INFORMACIÓN EN LAS CONTRATACIONES Y LAS RELACIONES CON LOS PORVEEDORES	67
8.8. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS BIENES Y EQUIPOS.....	69
8.9. SEGURIDAD DE LA INFORMACIÓN EN LOS PROCESOS MISIONALES.....	70
8.10. GESTIÓN JURÍDICA Y COMUNICACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	75
8.11. AUDITORÍA Y CONTROL DISCIPLINARIO	76
9. COMPROMISOS DE LA ALTA DIRECCIÓN	76
9.1. COMPROMISOS Y LIDERAZGO DE LA ALTA DIRECCIÓN	77
10. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN	78
11. ASPECTOS GENERALES	78
12. REVISIÓN Y APROBACIÓN.....	80
Anexo 1. Relación de cumplimiento ISO/IEC 27001:2013 - FGN.....	81
Anexo 1.1. Relación de cumplimiento ISO/IEC 27001:2013 – Procesos del Sistema	81
Anexo 1.2. Relación de cumplimiento de los controles del anexo A de la ISO/IEC 27001:2013	82
Anexo 1.3. Anexo A ISO/IEC 27001:2013	89
Anexo 2. Políticas y directrices de seguridad de la información.....	101


	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 4 de 111

INTRODUCCIÓN

La información es un activo valioso en las organizaciones, que puede verse expuesta a diversas amenazas como hurto, duplicación, adulteración, destrucción o pérdida, independientemente del medio de soporte en el que se encuentre (impreso o digital), razón por la cual la Fiscalía General de la Nación (FNG en adelante), a través de la Dirección de Planeación y Desarrollo por medio del Sistema de Gestión Integral SGI y de la Subdirección de Tecnologías de la Información y las comunicaciones, dando cumplimiento a las funciones otorgadas mediante el decreto Ley 898 de 2017, en lo referente a Seguridad y Privacidad de la Información, emite el presente documento por el cual se define y desarrolla el Sistema de Gestión de Seguridad y Privacidad de la Información y Seguridad Digital (SGSISD en adelante), en alineación con la política de seguridad y privacidad de la información adoptada por la entidad; de esta manera se asegura la confidencialidad, integridad y disponibilidad de la información generada por, o en custodia de la entidad.

Así mismo, teniendo en cuenta que los sistemas de seguridad y privacidad de la información y de seguridad digital tienen estrecha relación con la informática, la archivística y la tecnología, y con base en las buenas prácticas de la familia de normas ISO/IEC 27000 y el MSPI del MinTIC, a través del presente documento se desarrollan un conjunto de políticas y lineamientos que definen y estandarizan el uso, control y apropiación del SGSISD en todos los niveles y áreas de la entidad; que de manera articulada con el sistema de gestión integral SGI, garantiza su diseño, implementación, seguimiento y control, y mejora continua en la gestión por procesos.

En consecuencia, el presente documento formaliza el compromiso de la Alta Dirección y desarrolla la Política General de Seguridad de la Información de la FGN, por la cual se definen los roles y responsabilidades para su implementación y apropiación en la entidad

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 5 de 111

1. OBJETIVO

Establecer la documentación, los lineamientos, políticas y directrices, y la metodología para el diseño, desarrollo y despliegue del Sistema de Gestión de Seguridad de la Información y Seguridad Digital SGSISD de la FGN, en todos los procesos y niveles de la Entidad.

2. ALCANCE

El alcance del presente Manual y de los documentos, lineamientos, políticas y directrices que se desarrollen a partir de éste, serán de obligatoria aplicación para todos los procesos y niveles de la entidad, así como para los servidores y funcionarios de la FGN, usuarios internos y externos, judicantes, practicantes, proveedores, contratistas, prestadores de servicios de la entidad ya sean públicos o privados, y cualquier otro que en cumplimiento de sus funciones o de sus obligaciones contractuales tenga acceso de cualquier nivel a los activos de información de la FGN¹.

3. DEFINICIONES Y SIGLAS.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.²

Activo de información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.³


Nota. Activo de información y recursos, se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.⁴

¹ Activo de información: todo lo que tenga valor para la entidad y que se encuentre dentro del inventario de activos de información como aplicaciones para trámites o servicios, sistemas de información, plataforma tecnológica, infraestructura física, cualquier tipo de documentación física o digital desde la que se genere, obtenga, adquiera, transforme o controle información en la que la entidad se encuentre como sujeto obligado por la ley 1581 de 2012, ley 1712 de 2014, decreto 1377 de 2013, o cualquier ley, decreto o norma gubernamental que los reglamente o complemente.

² <https://www.iso27000.es/glosario.html>

³ Modelo de Seguridad y Privacidad de la Información, MINTIC. Anexo 1 - 2016.

⁴ Modelo de Seguridad y Privacidad de la Información, MINTIC. Anexo 1 – 2021 (CONPES 3854 de 2016).

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 6 de 111

- **Activo crítico:** La FGN define como activo crítico, a todos y únicamente, a los activos de información y digitales que se encuentren declarados dentro de la *Matriz de Registro de Activos de Información de la FGN*, y que después de la valoración de confidencialidad, integridad o disponibilidad, quede con un “*nivel de criticidad alto o medio*”; o que, después de la evaluación de valor de recuperación y de nivel de afectación en el desarrollo de las actividades de los procesos, quede con un “*nivel de importancia para la entidad de: activo de muy alto valor o activo de alto valor*”.

Nota. Para mayor comprensión, dentro del SGI se desarrolla la *Guía para la administración y gestión de riesgos y controles de seguridad de la información y seguridad digital*, el *Formato matriz de registro de activos de información de la FGN* y la demás documentación que los complementa.

Acuerdo de Confidencialidad: Documento donde el servidor, contratista, practicante o tercero se compromete a no divulgar, usar o explotar la información a beneficio propio o de terceros debido al acceso a la información como consecuencia de la labor que desempeñan en la FGN.

Alcance: (Inglés: Scope). Ámbito de la organización que queda sometido al SGSISD.⁵

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.⁶

Archivística: Ciencia que se encarga del estudio teórico y práctico de los principios, procedimientos y problemas concernientes al almacenamiento de documentos, físicos o digitales, buscando que dicha documentación (información y datos) se mantenga en el tiempo y pueda ser consultada, conservando su trazabilidad (metadatos).

Autenticación: Provisión de una garantía de que una característica afirmada por una entidad es correcta


[Fuente: ISO/IEC 27002:2015 numeral 10.1.1, literal d.] ... “*uso de técnicas criptográficas para autenticar usuario y otras entidades del sistema que solicitan acceso a usuarios, entidades o recursos del sistema, o tener tracciones con ellos.*” ...

Autenticidad: Propiedad de que una entidad es lo que afirma ser.⁷

⁵ <https://www.iso27000.es/glosario.html>

⁶ *Ibidem*

⁷ *Ibidem*

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 7 de 111

COLCERT: Grupo⁸/Equipo de Respuesta a Emergencias Cibernéticas de Colombia, su finalidad es asesorar, apoyar y coordinar a las múltiples partes interesadas para la adecuada gestión de los riesgos e incidentes digitales. Es el punto único de contacto y respuesta nacional que coopera y ayuda a responder de forma rápida y eficiente a los incidentes de seguridad digital y a gestionar de forma activa las amenazas de seguridad digital, incluyendo la coordinación a nivel nacional e internacional de las distintas capacidades de respuesta a incidentes o Centros de Operaciones de Seguridad Digital existentes.⁹

Competencia: Capacidad de aplicar conocimientos y habilidades para lograr los resultados previstos.¹⁰

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados¹¹. Contiene el atributo de privacidad.

Continuidad de la seguridad de la información: Procesos y procedimientos para garantizar una “operativa continuada” -continuidad en la operación- de la seguridad de la información.¹²

Control: Medida por la que se modifica el riesgo.

[Fuente: ISO Guía 73:2009] ...“*Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguardan o contramedida son utilizados frecuentemente como sinónimos de control.*”

Control de acceso: Significa garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad.¹³

Criptografía: Técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet.¹⁴

CSIRT: (Computer Security Incident & Response Team) Equipo de Respuesta a Incidentes de Seguridad Cibernética, por su sigla en inglés. Es el equipo que provee

⁸ <https://www.colcert.gov.co/800/w3-channel.html>

⁹ Artículo 2.2.21.1.5.2. Equipo de Respuesta a Emergencias Cibernéticas de Colombia. Decreto 338 de 2022


¹⁰ <https://www.iso27000.es/glosario.html>

¹¹ *Ibidem*

¹² Modificado de la definición entregada por la ISO 27000, <https://www.iso27000.es/glosario.html>

¹³ <https://www.iso27000.es/glosario.html>

¹⁴ <https://tecnologia-informatica.com>

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 8 de 111

las capacidades de gestión de incidentes a una organización/sector en especial. Esta capacidad permitir minimizar y controlar el daño resultante de incidentes, proveyendo la respuesta, contención y recuperación efectiva, así como trabajar en pro de prevenir la ocurrencia de futuros incidentes.¹⁵

Custodio: El custodio tanto técnico como funcional es un cargo (persona o servidor público que lo ocupa), grupo de trabajo o proceso de la FGN, encargado de administrar y hacer efectivos los controles definidos en la gestión de riesgos de seguridad de la información y seguridad digital, y su declaración de aplicabilidad.¹⁶

- [Guía no. 5 del MSPI del MinTIC] Custodio es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado, entre otros que defina la entidad.
- [ISO/IEC 27002:2015, numeral 8.1.2 “Propiedad de los activos”] Las tareas de rutina pueden ser delegadas, por ejemplo, a un custodio que velará por los activos diariamente, pero la responsabilidad sigue siendo de los propietarios.
- [Anexo 1 del MSPI del MinTIC, febrero del 2021] El custodio es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario. (Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los custodios pueden ser los funcionarios o el proceso de archivo o correspondencia, el custodio generalmente se define donde reposa el activo original).


Declaración de aplicabilidad: (Inglés: Statement of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la organización - tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO/IEC 27001.¹⁷

Directriz: Para el SGSISD de la FGN, son aquellas normas con el peso de políticas de SI que se deben implementar para alcanzar los objetivos del sistema,

¹⁵ Artículo 2.2.21.1.1.3. Definiciones. Decreto 338 de 2022.

¹⁶ Adaptado de ISO/IEC 27002:2013.

¹⁷ <https://www.iso27000.es/glosario.html>

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 9 de 111

identificadas dentro del número 5.1.1 de la *Guía de Implementación ISO/IEC 27002:2015*. Son una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos¹⁸.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad, persona, proceso u área autorizada.¹⁹

Evaluación de riesgos: (inglés: Risk assessment). Proceso global de identificación, análisis y estimación de riesgos. [Fuente: ISO Guía 73:2009].²⁰

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias.

[Fuente: ISO Guide 73: 2009] ... *“Un evento puede ser una o más ocurrencias y puede tener varias causas. Un evento puede consistir en que algo no suceda. Un evento a veces puede ser referido como un “incidente” o “accidente”.”* ...

Evento de seguridad de la información: Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.²¹

Gestión de incidentes de seguridad de la información: (inglés: Information security incident management). Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información²².

Identificación de riesgos: Proceso de encontrar, reconocer y describir riesgos [Fuente: Guía ISO 73:2009].

La identificación de riesgos implica la identificación de las fuentes del riesgo, eventos, sus causas y sus posibles consecuencias. La identificación de riesgos puede involucrar datos históricos, análisis teóricos, opiniones informadas y de expertos, y las necesidades de las partes interesadas.²³

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una

¹⁸ <https://www.iso27000.es/glosario.html>


¹⁹ *Ibidem*

²⁰ *Ibidem*

²¹ *Ibidem*

²² *Ibidem*

²³ *Ibidem*

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 10 de 111

probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.²⁴

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.²⁵

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.²⁶

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados. consagrados en el artículo 18 de esta ley.²⁷

Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.²⁸

Informática: Conjunto de conocimientos técnicos que se ocupan del tratamiento automático de la información por medio de computadoras.

Integridad: Propiedad de la información relativa a su exactitud y completitud.²⁹

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSISD, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos³⁰.

²⁴ <https://www.iso27000.es/glosario.html>

²⁵ Ley No. 1712 de 2014: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".


²⁶ Inciso b), Artículo 6. Definiciones de la Ley 1712 de 2014.

²⁷ Inciso c), Artículo 6. Definiciones de la Ley 1712 de 2014

²⁸ Inciso d), Artículo 6. Definiciones de la Ley 1712 de 2014

²⁹ <https://www.iso27000.es/glosario.html>

³⁰ *Ibidem*

 FISCALÍA <small>GENERAL DE LA NACIÓN</small>	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 11 de 111

ISO/IEC 27001: Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSISD). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSISD a nivel mundial.³¹

ISO/IEC 27002: Código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable.³²

Legalidad: Se refiere al uso legal de programas de computación protegiendo entre otros el derecho de propiedad intelectual; garantiza la no utilización de copias de software no autorizadas y/o piratería.

MGRSD: Modelos de gestión de riesgos de seguridad digital del MinTIC.

Monitoreo: Determinar el estado de un sistema, un proceso o una actividad. Para determinar el estado, puede ser necesario verificar, supervisar u observar críticamente.³³

MSPI del MINTIC: Modelo de seguridad y privacidad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

No repudio: Capacidad de probar la ocurrencia de un evento o acción reclamada y sus entidades de origen.³⁴ Hace referencia a la irrenunciabilidad y está relacionado con un servicio de seguridad con el cual prueba la participación de las partes en una comunicación: una para el emisor que se entiende por el origen y con este el emisor no podrá negar que envió porque el destinatario tiene pruebas del envío. Por otro lado, está el destino que en este caso es el receptor el cual no podrá negar el recibo del mensaje por que el emisor tiene pruebas de la recepción.


[Fuente ISO/IEC 27002:2015 numeral 10.1.1 literal c.] ... *“No-repudio es el uso de técnicas criptográficas para suministrar evidencia de que un evento o acción ocurre o no ocurre.”* ...

³¹ <https://www.iso27000.es/glosario.html>

³² *Ibidem*

³³ *Ibidem*

³⁴ *Ibidem*

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 12 de 111

Según [CCN-STIC-405:2006] ... *“El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.”* ...

Según [OSI ISO-7498-2] No repudio ... *“Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).”* ...

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.³⁵

Política: Intenciones y dirección de una organización, expresada formalmente por su alta dirección.³⁶

Política de escritorio limpio: (inglés: Clear desk policy). La política de la empresa que indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.³⁷

Propietario de la Información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.³⁸


- [Guía no. 5 del MSPI del MinTIC] Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso
- [Guía no. 4 del MSPI del MinTIC – MGRSD] Identificar el dueño de los activos: Cada uno de los activos identificados deberá tener un dueño designado, si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.

³⁵ <https://www.iso27000.es/glosario.html>

³⁶ *Ibidem*

³⁷ *Ibidem*

³⁸ Adaptado de ISO/IEC 27002:2013

 FISCALÍA <small>GENERAL DE LA NACIÓN</small>	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 13 de 111


- [Anexo 1 del MSPI del MinTIC, febrero del 2020] Los propietarios y custodios de la información producida en el área, deben identificar, clasificar y valorar los activos de información de acuerdo con la siguiente compilación de Activos de Información teniendo en cuenta lo establecido en la norma técnica ISO/IEC 27000: (Información; Software como programa informático; Hardware como computadora; servicios; personas, y sus calificaciones, habilidades y experiencia; intangibles como reputación e imagen).
- [ISO/IEC 27002:2015, numeral 6.1.1 “Roles y Responsabilidades] Se debe nombrar un propietario para cada activo, quien entonces se convierte en el responsable de su protección diaria.
- [ISO/IEC 27002:2015, numeral 8.1.2 “Propiedad de los activos”] Se asegurará la asignación oportuna de los propietarios de los activos. La propiedad se asigna cuando los activos son creados o transferidos. El propietario del activo deberá ser responsable de su *“GESTIÓN DURANTE TODO SU CICLO DE VIDA”*.
- [ISO/IEC 27005:2020, numeral 8.2.2 “Identificación de Activos”] Para el inicio de identificación de riesgos se debe levantar el inventario de activos con su propietario, ubicación, función, entre otros.
- [ISO/IEC 27001:2013, control A.8.1.2 “Propietario de los activos”] Los activos mantenidos en el inventario deberían tener un propietario.
- [ISO/IEC 27001:2013, control A.9.2.5. “Revisión de los derechos de acceso de usuario”] Los propietarios de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.³⁹

Profesional del sistema de gestión de seguridad de la información: Persona que establece, implementa, mantiene y mejora continuamente uno o más procesos del sistema de gestión de seguridad de la información.⁴⁰

³⁹ <https://www.iso27000.es/glosario.html>

⁴⁰ *Ibidem*

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 14 de 111

Propietario del riesgo: (inglés: Risk owner). Persona o entidad con responsabilidad y autoridad para gestionar un riesgo [Fuente: ISO Guide 73:2009].⁴¹

Riesgo: Efecto de la incertidumbre sobre los objetivos.⁴²

Nota.

1. Un efecto es una desviación de lo esperado: positivo o negativo.⁴³
2. La incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o probabilidad.⁴⁴

... *“El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.”*⁴⁵ ...

Seguridad de la Información (SI): Preservación de la confidencialidad, integridad y disponibilidad de la información.⁴⁶

... *“Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas.”*⁴⁷ ...

Sistema de Gestión Integral (SGI): Corresponde a la herramienta de planeación y gestión de la Fiscalía General de la Nación que tiene como propósito establecer, articular, implementar, controlar y mejorar continuamente la gestión institucional, atendiendo al uso del enfoque basado en procesos, la práctica estratégica de arquitectura institucional, el pensamiento basado en riesgos y la satisfacción de los usuarios, con el fin de que todas las actividades, operaciones y actuaciones se realicen con transparencia, integridad y legalidad, de acuerdo con la reglamentación vigente, las normas, las políticas de gestión y desempeño aplicables así como las metas y objetivos trazados por la alta dirección en el marco de las instancias de gobierno, a través de la adopción de buenas prácticas e implementación de estándares y normas técnicas.⁴⁸

⁴¹ <https://www.iso27000.es/glosario.html>

⁴² *Ibidem*

⁴³ *Ibidem*


⁴⁴ *Ibidem*

⁴⁵ *Ibidem*

⁴⁶ *Ibidem*

⁴⁷ *Ibidem*

⁴⁸ Definiciones y siglas, Procedimiento para la Creación, Actualización y Control de la Información Documentada FGN-SP01-P-01 V06.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 15 de 111

Sistema de Gestión de la Seguridad de la Información: (inglés: Information Security Management System). Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.⁴⁹

Sistema de Información: Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes que manejan información.⁵⁰

SubTIC: Subdirección de Tecnologías de la Información y las Comunicaciones de la Fiscalía General de la Nación.

Tecnología: Conjunto de instrumentos, recursos técnicos o procedimientos empleados en un determinado campo o sector.

Nota. Todas las demás siglas y definiciones contenidas en la norma ISO/IEC 27000 y en el modelo de seguridad y privacidad de la información MSPI del MinTIC y su anexo 1.


Teletrabajo: Una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios utilizando como soporte las tecnologías de la información y comunicación -TIC- para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo" (Artículo 2, Ley 1221 de 2008).

Trabajo remoto o trabajo en casa: Ley 2121 de 2021, "Por la cual se crea el régimen de trabajo remoto".

Usuario de la Información: Cualquier servidor o tercero, que haya sido autorizado por el propietario de la información para el uso, procesamiento, tratamiento, manejo o acceso a ésta.


⁴⁹ <https://www.iso27000.es/glosario.html>

⁵⁰ *Ibíd*em

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 16 de 111

4. MARCO LEGAL / DOCUMENTOS DE REFERENCIA


- Ley 1266 de 2007, *“Por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales”*.
- Ley 1581 de 2012, *“Protección de Datos personales”*.
- Decreto 1377 de 2013, *“Por la cual se reglamenta parcialmente la Ley 1581 de 2012”*
- Decreto – Ley 016 de 2014, *“Por el cual se modifica la estructura orgánica de la Fiscalía General de la Nación”*, modificado por el decreto 898 de 2017.
- Ley 1712 de 2014, *“Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”*.
- Decreto 103 de 2015, *“Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014, y se dictan otras disposiciones”*.
- Decreto 1083 de 2015, *“Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”*.
- Decreto 612 de 2018. *“Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”. [...] Artículo 1: ... 11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. 12. Plan de Seguridad y Privacidad de la Información.*
PARÁGRAFO 1. La integración de los planes mencionados en el presente artículo se hará sin perjuicio de las competencias de las instancias respectivas para formularlos y adoptarlos. [...]
- Decreto 2106 de 2019, *“Por el cual se establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones”*.
- Decreto 338 de 2022, *“Lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el modelo y las instancias de Gobernanza de Seguridad Digital”*.
- Resolución 4004 de 2013, *“Política de Seguridad Informática de la Fiscalía General de la Nación”*.
- Resolución 1261 de 2014, *“Buenas prácticas para el desarrollo, mantenimiento y calidad de los sistemas de información de la FGN”*.
- Resolución 1704 de 2014, *“Por la cual se establecen las políticas generales de Seguridad Física en Fiscalía General de la Nación”*.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 17 de 111

- Resolución No.1165 de 2018: *“Por la cual se crea el esquema de Arquitectura Institucional de la Fiscalía General de la Nación”*.
- Resolución 0-1400 septiembre de 2021 *“Por medio de la cual se establecen las Instancias de Gobierno en la Fiscalía General de la Nación, se fortalece el Sistema de Gestión Integral, el Sistema de Control Interno, se adopta la práctica estratégica de Arquitectura Institucional y se dictan otras disposiciones”*
- Resolución 005 diciembre de 2021 *“Por medio de la cual se adopta la versión 01 del Manual de Arquitectura Institucional de la Fiscalía General de la Nación dentro del Proceso Planeación Estratégica”*.

4.1. OTROS DOCUMENTOS DE REFERENCIA

- Directiva Presidencial 002 de 2022. Reiteración de la Política Pública en materia de Seguridad Digital.
- CONPES 3701 de 2011. Lineamientos de Política para Ciber-seguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad Digital.
- CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital.
- Anexo 3 – Resolución 1519 agosto de 2020 del MinTIC *“Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos”*.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5, Departamento de la Función Pública, noviembre de 2020.
- Anexo 1 - Modelo de Seguridad y Privacidad de la Información, Documento maestro versión 4.0, febrero del 2021.
- Resolución 00500 del Ministerios de Tecnologías de la Información y las Comunicaciones MinTIC, marzo 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”*.
- Modelo de Seguridad y Privacidad de la Información, MINTIC, 2016.
- Norma Técnica ISO/IEC 27000 Tecnología de la información.
- Norma Técnica Colombiana ISO/IEC 27001:2013 Sistemas de Gestión de Seguridad de la Información. Requisitos.
- Norma Técnica ISO/IEC 27002:2015 Código de practica para controles de seguridad de la información.
- ISO/IEC 27005:2020. *Gestión de Riesgo*.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 18 de 111

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Fiscalía General de la Nación adopta la Política de Seguridad de la Información por medio de la Resolución 4004 del 6 de noviembre del 2013, *“por la cual se actualizan las políticas de seguridad de la información, emitidas mediante circular DFGN – 0001, mayo 6 de 2006 del Fiscal General de la Nación”*.

5.1. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA FGN

“La política de seguridad informática tiene por objeto proteger los activos informáticos de la Fiscalía General de la Nación y garantizar un adecuado uso de la tecnología, ante amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información.”⁵¹


5.2. ALCANCE DE LA POLÍTICA

“La Política General de Seguridad Informática establece los lineamientos de gestión adecuada para el uso de los activos de información de la entidad, asegurando la implementación de los controles y medidas de seguridad formuladas en esta política a partir de la identificación de los activos de información, las partidas presupuestarias correspondientes y el cumplimiento de las disposiciones legales vigentes

Por tal razón, esta Política debe ser continuamente actualizada de acuerdo con los procesos, procedimientos, instructivos y actividades establecidos de la entidad, a efectos de asegurar su vigencia y nivel de eficacia, así como conocida y cumplida por todos los usuarios de los activos de información, es decir servidores, contratistas y terceras personas que de alguna forma tenga acceso a los recursos informáticos de la Fiscalía General.

Lo anterior en coherencia con las normas planteadas en este documento (resolución 4004 del 2013) y con las Políticas de Seguridad Informática elaboradas en el marco de la norma técnica NTC ICO/IEC 27001, así como con los documentos de procedimientos y recomendaciones que se han publicado y formalizado mediante

⁵¹ Resolución 4004 del 6 de noviembre de 2013, artículo primero. Objetivo.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 19 de 111

*Resolución 2287 el 5 de noviembre de 2003, y de los lineamientos del SGC y MECI.*⁵²

6. MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA FISCALÍA GENERAL DE LA NACIÓN

Fiscalía General de la Nación adopta un modelo de gestión de seguridad de la información propio, basado en el MSPI del MinTIC y la familia de normas ISO/IEC 27000, el cual se aterriza a través del Sistema de Gestión de Seguridad de la Información y seguridad Digital (SGSISD en adelante); su eje central se encuentra en la Política General de Seguridad de la Información (Política General de SI en adelante), que se adecua y actualiza a través del presente Manual y de las políticas y lineamientos de seguridad de la información y seguridad digital desarrolladas desde los diferentes procesos del SGI.

Cuenta con un modelo de administración y gestión de riesgos y controles de seguridad de la información y seguridad digital, para los activos críticos identificados en la Matriz de Registro de Activos de Información de la FGN y que se debe adoptar en todos los niveles, áreas y procesos de la FGN, en conjunto con la declaración de aplicabilidad de la Política General de SI.

⁵² Resolución 4004 del 6 de noviembre de 2013, artículo segundo. Alcance.


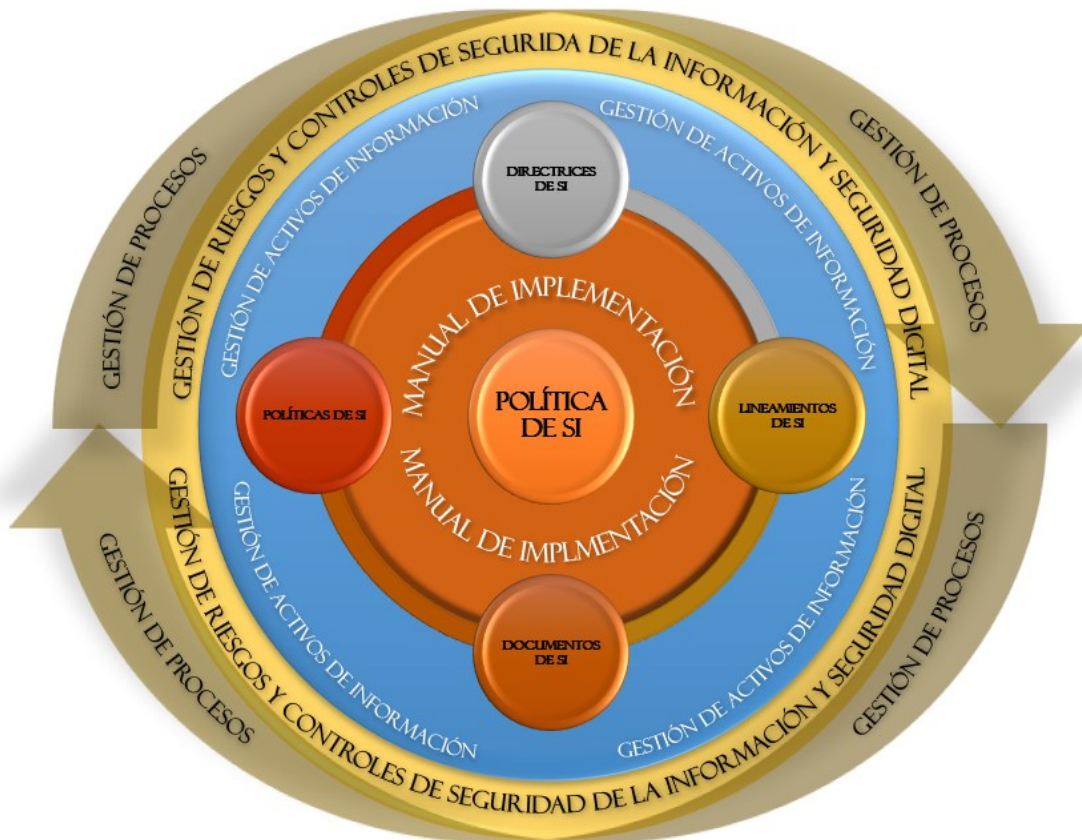
	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 20 de 111

Ilustración 1 Modelo de Gestión de Seguridad de la Información de la FGN.




Fuente. Dirección de Planeación y Desarrollo

6.1. CICLO DE OPERACIÓN DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El ciclo de operación de Modelo de Gestión de Seguridad de la Información de la FGN (MGSI en adelante) consta de cuatro fases, iguales a las del ciclo PHVA⁵³ de mejora continua, pero acondicionado del MSPI del MinTIC para el SGI de la FGN, de tal forma que inicia con el plan de implementación y finaliza con su ajuste.

Dentro de las cuatro fases existen momentos, que se desarrollan entre la finalización de una y el inicio de la otra, lo que permite afianzar la efectividad del

⁵³ PHVA: Planear, hacer, verificar, actuar.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 21 de 111

ciclo de operación; estos, son actividades que al ejecutarse dan estabilidad al MGSI antes de continuar con la siguiente fase del ciclo de operación.

➤ **Fases**

- Primera fase “Plan de implementación”: periodo de planificación del SGSISD y de su alineación con el Direccionamiento Estratégico y el Sistema de Gestión Integral.
- Segunda fase “Operación del SGSISD”: fase en la que se materializan todas las actividades y propuestas planteadas en la primera fase.
- Tercera fase “Seguimiento”: etapa en la que se evalúan los resultados obtenidos de la operación y su tiempo de maduración o momento de operatividad.
- Cuarta fase “Ajuste al plan”: actividades a desarrollar para corregir desviaciones encontradas al plan original, y plantear las propuestas para la mejora de SGSISD y del plan de continuidad de negocio.

➤ **Momentos**

- Primer momento “Diagnóstico SGSISD”: entre las fases del plan de implementación y operación de SGSISD, con el fin de establecer el nivel de los controles de seguridad de la información y seguridad digital que operan actualmente y el Plan de Tratamiento de Riesgos (en adelante PTR) a implementar.
- Segundo momento “Operatividad de SGSISD”: tiempo de maduración entre las fases de operación de sistema y seguimiento, la misma no debería ser menor a un año después de finalizada la fase de operación o de cada una de sus etapas de implementación.
- Tercer momento “Revisión SGSISD”: espacio entre las fases de seguimiento y ajuste al plan del SGSISD, en donde se evaluarán los resultados del seguimiento realizado a la fase de operación y se realiza la revisión por la Alta Dirección.
- Cuarto momento “Ajuste SGSISD”: conforman el conjunto de propuestas resultantes de la fase de ajuste al plan del SGSISD y su alineación con los procesos que las aterrizarán e implementarán.


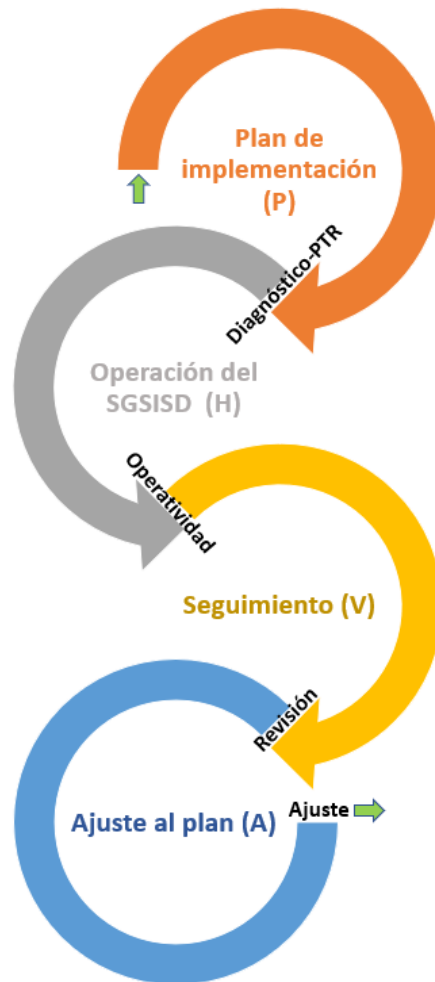
	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 22 de 111

Ilustración 2 Secuencia de las fases y los momentos del ciclo de operación.




Fuente. Dirección de Planeación y Desarrollo

6.2. DESARROLLOS DE LAS FASES DEL CICLO DE OPERACIÓN DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA FGN

6.2.1. Primera fase “Plan de Implementación”

La primera fase del ciclo de operación del MGSi es el *plan de implementación*, corresponde al *planear* (P) del ciclo de mejora continua y en él se establecen las bases del SGSISD, los límites de operación y las metas a cumplir; tiene como productos:


	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 23 de 111

- 1) Política General de SI de la FGN definida, revisada y/o actualizada.
- 2) Alcance del SGSISD.
- 3) Contexto y caracterización de seguridad de la información y seguridad digital de la entidad.
- 4) Objetivos del SGSISD.
- 5) Roles y responsabilidades de seguridad de la información y seguridad digital.
- 6) Plan de implementación del SGSISD que contenga:
 - Cronograma de desarrollo de las fases y momentos del ciclo de operación y sus entregables.
 - Cronograma de comunicaciones, capacitación y apropiación del SGSISD.
 - Cronograma de levantamiento del registro de activos de información.
 - Cronograma de identificación y valoración de los riesgos de seguridad de la información y seguridad digital de la FGN.
 - Planteamiento y desarrollo de pruebas necesarias en todas las fases y momentos de ciclo de operación.
- 7) Registro de activos de Información de la FGN.
- 8) Metodología de registro de activos de información (inventario y clasificación).
- 9) Metodología de administración y gestión de riesgos y controles de seguridad de la información y seguridad digital.

6.2.2. Fase de Operación del SGSISD

La segunda fase del ciclo de operación del MGSi es *la operación del SGSISD*, corresponde al *hacer* (H) del ciclo de mejora continua y en él se lleva a cabo la implementación y ejecución de lo planteado en la primera fase y en el primer “momento” del ciclo de operaciones; en esta fase se encuentra en operación el sistema y se desarrollan las siguientes actividades:

- 1) Implementación y puesta en marcha del Plan de Tratamiento de los Riesgos -PTR- de seguridad de la información y seguridad digital de la FGN (implementación de requisitos y controles por proceso, consultar como referencia el anexo 1 de este documento).
- 2) Declaración de aplicabilidad de la Política aprobada por la Alta Dirección.
- 3) Manual de políticas de Seguridad de la Información.
- 4) Ejecución y seguimiento del plan de implementación.
- 5) Levantamiento, gestión y seguimiento de los indicadores de los riesgos de seguridad de la información y seguridad digital de la FGN.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 24 de 111

- 6) Seguimiento, evaluación y gestión de los controles de los riesgos de seguridad de la información y seguridad digital de la FGN.

6.2.3. Fase de Seguimiento

La tercera fase del ciclo de operación del MGSI es la fase de *seguimiento al SGSISD*, corresponde al *verificar (V)* del ciclo de mejora continua y en él se desarrollan las actividades necesarias para evaluar en nivel de implementación del SGSISD, en cumplimiento de sus objetivos y de los requisitos del anexo A de la ISO/IEC 27001:2013⁵⁴, por lo que en esta fase se realizará:

- 1) Seguimientos a la primera y segunda fase del ciclo de operación del MGSI de la FGN, una vez finalizado el segundo “momento” del ciclo de operación.
- 2) Revisión del SGSISD
 - Conformidad y cumplimiento del alcance, objetivos, documentación y políticas, directrices y lineamientos de SI.
 - Implementación de lineamientos y requisitos en los procesos y sus resultados.
 - Conformidad de la Política General de SI.
 - Revisión de resultados de la gestión de riesgos, indicadores y controles.
 - Conformidad del plan de tratamiento de riesgos de seguridad de la información -PTR-.
- 3) Revisión del Plan de implementación del SGSISD.


Nota. Los anteriores, son los aspectos sugeridos a evaluar dentro de la fase de seguimiento del ciclo de operación, sin embargo, es de autonomía de quien realice el seguimiento o revisión el escoger dichos aspectos, siempre y cuando no se encuentren por fuera del alcance y los objetivos del SGSISD y se realice conforme con las disposiciones del SGI de la FGN.

6.2.4. Ajustes al Plan del SGSISD

La cuarta fase del ciclo de operación del MGSI es la fase de *seguimiento al SGSISD*, corresponde al *actuar (A)* del ciclo de mejora continua y es la fase en la que se realizan los ajustes del “plan de implementación”; se analizan los resultados de la fase de seguimiento y del “momento de revisión” y se establecen las metas y cambios para el nuevo inicio del ciclo de operación:

- 1) Plan anual de mejora del SGSISD.
 - Planes de mejoramiento.
 - Plan de continuidad del SGSISD.

⁵⁴ El anexo A de la norma ISO/IEC 27001:2013, se puede consultar en el anexo 1.3 de este documento.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 25 de 111

- 2) Acciones correctivas.
- 3) Resultados de la revisión por la Alta Dirección.
- 4) Otros.

6.3. DESARROLLO DE LOS MOMENTOS DEL CICLO DE OPERACIÓN DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA FGN.

6.3.1. Momento de Diagnóstico y PTR

El primer momento del ciclo de operación del MGSi de la FGN, es el “momento de diagnóstico y PTR”, por ser la etapa del ciclo de operación en la que se realiza el diagnóstico de los controles de SI existentes, implementados y su estado de funcionamiento, eficiencia y eficacia con respecto a los riesgos de seguridad de la información y seguridad digital identificados de los activos críticos; con base en los resultados del diagnóstico de controles de SI, se plantea el Plan de Tratamiento de Riesgo de Seguridad de la Información y Seguridad Digital de la FGN o PTR.

Este momento se lleva a cabo entre las fases del ciclo de operación “plan de implementación” y “operación del SGSISD”; sin la entrega satisfactoria del diagnóstico de controles de SI y la aprobación, parcial o por etapas, del Plan de Tratamiento de Riesgos de Seguridad de la Información y Seguridad Digital de la FGN o PTR, no se podrá iniciar la fase de “operación del SGSISD”.


Nota. Para el desarrollo del diagnóstico, se puede usar la herramienta de autodiagnóstico del MSPI del MinTIC, u otra que cubra las necesidades de la entidad y los requisitos de las normas ISO/IEC 27000.

Cada actividad del El Plan de Tratamiento de Riesgos de Seguridad de la Información y Seguridad Digital de la FGN o PTR, deberá tener la aprobación del propietario del activo objeto de control⁵⁵; incluirá, los controles a implementar, las actividades, fechas y responsables de implementación y su correspondiente presupuesto.

Para que el PTR entre a operar, deberá estar aprobado o tener aprobación parcial o por etapas del Comité Gestión de la FGN, previo visto bueno de la Mesa Técnica Operativa de Arquitectura Institucional.

Nota. Las dependencias que tengan dentro del PTR aprobado, la adquisición de elementos de control para la mitigación de los riesgos, deben incluir, si se requiere, dicha necesidad dentro de su plan anual de adquisiciones Plan Anual de Adquisiciones – PAA toda vez que la responsabilidad de

⁵⁵ Decreto 612 de 2018 Publicación antes de 31 de enero de cada vigencia.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 26 de 111

la implementación de la seguridad de la información es de toda la entidad y no exclusiva de la Subdirección de TIC o de la Dirección de Planeación y Desarrollo.

6.3.2. Momento de Operatividad del SGSISD

El segundo momento del ciclo de operación del MGSI de la FGN, es el “momento de operatividad del SGSISD”, corresponde al periodo de maduración requerido para la obtención de los resultados a partir de la fase de operación. Está determinado por el tiempo propuesto en el cronograma del PTR, para la implementación de los controles.

Nota. El paso a la fase de “seguimiento”, no puede ser menor al tiempo establecido en el cronograma del PTR y a al tiempo definido para la medición de los indicadores de los riesgos que permitan evidenciar el estado de estos después de controles.

Por lo anterior, el momento de operatividad corresponde únicamente al tiempo de maduración del sistema, por lo que, este momento es individual para cada actividad a implementar en la “fase de operación SGSISD” y su tiempo de maduración para la obtención de resultados, sin el vencimiento del tiempo, no se dará a inicio a la siguiente “fase de seguimiento de SGSISD”.

6.3.3. Momento de la Revisión del SGSISD


El tercer momento del ciclo de operación del MGSI de la FGN, es el “momento de revisión del SGSISD”; en este momento se analizan los resultados obtenidos en la fase de seguimiento, los datos arrojados por lo resultados, las desviaciones al alcance de los objetivos, las metas no alcanzadas, los incumplimientos encontrados a los requisitos, la revisión a la implementación del plan de implementación de SGSISD y se prepara y presenta la revisión por la Alta Dirección.

Las métricas, estadísticas y datos obtenidos de los resultados, serán el insumo para iniciar la “fase de ajustes al plan del SGSISD”.

Nota. Se verificará que se hayan revisado y hecho seguimiento a todos los elementos que conforman del SGSISD; de haber hecho falta alguno, se deberá hacer el respectivo seguimiento en este “momento”.

6.3.4. Momento de Ajuste al SGSISD

El cuarto momento del ciclo de operación del MGSI de la FGN, es el “momento de ajustes del SGSISD”; este es el espacio de revisión de las propuestas planteadas en la “fase de ajuste al plan SGSISD”, es el momento de revisar que el plan anual de mejora esté ajustado a los objetivos y metas estratégicas, y que los objetivos, las metas, los proyectos y demás actividades planteadas, estén acorde con la realidad, los recursos y el estado de la Entidad.

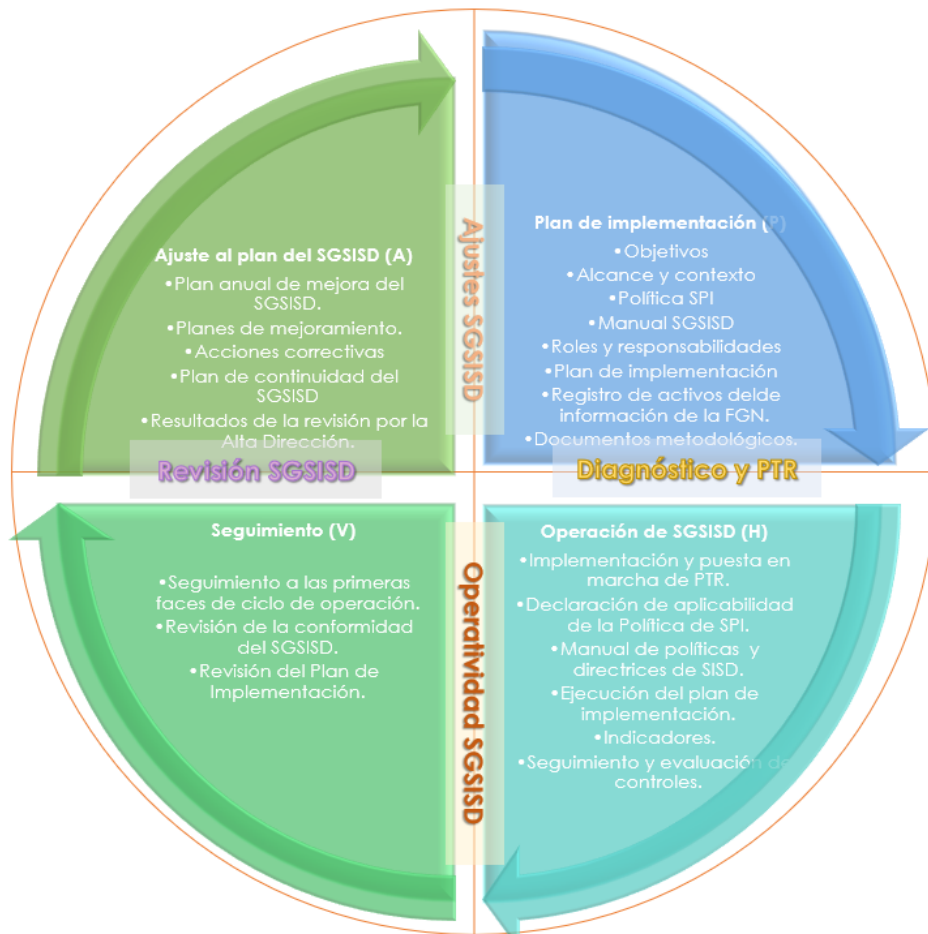
	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 27 de 111

También se revisa que los objetivos, las metas, los proyectos y demás actividades descritas en los procesos, estén planteadas de la manera adecuada para subsanar las desviaciones encontradas en la fase de seguimiento, con el objeto de alcanzar las metas, el mantenimiento y el desarrollo del sistema, de lo contrario, se deberán replantear para que sean objetivas y alcanzables.


6.4. ESQUEMA DEL CICLO DE OPERACIÓN DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MGSÍ DE LA FGN.

El ciclo de operación del MGSÍ de la FGN, es a su vez el ciclo de mejora continua del SGSISD, las cuatro fases y los cuatro momentos que lo conforman se representan en la siguiente imagen:

Ilustración 3 Ciclo de operación del MGSÍ de la FGN.



Fuente. Dirección de Planeación y Desarrollo

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 28 de 111

7. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL (SGSISD)

El Sistema de Gestión de Seguridad de la Información y Seguridad Digital -SGSISD- es un modelo de gestión basado en las buenas prácticas de la familia de normas ISO/IEC 27000 y MSPI del MinTIC, que asegura la confidencialidad, integridad y disponibilidad de la información que la Entidad genere, obtenga, adquiera, transforme, controle o custodie, presente o almacenada en medios físicos o digitales.


Basado en la aplicación en todos los niveles, áreas y procesos de la entidad, de un esquema de administración de riesgos de SI, que permita gestionar, evaluar, monitorear y controlar todos los posibles eventos que amanecen la confidencialidad, privacidad, integridad y disponibilidad de la información (datos y los activos de información).

7.1. OBJETIVO

Gestionar la seguridad de la información física o digital, generada, obtenida o transformada por la entidad; controlando la confidencialidad, integridad, disponibilidad y privacidad de los activos de información en todo su ciclo de vida y la protección de sus activos asociados ante cualquier amenaza interna o externa, deliberada o accidental, asegurando la continuidad de los servicios que soportan el cumplimiento de la misión y el propósito de la Entidad, dentro de un ciclo de mejora continua.

7.1.1. Objetivos específicos

- 7.1.1.1.** Establecer un sistema de seguridad y privacidad de la Información y de seguridad digital, desarrollado con base en los lineamientos aplicables a la FGN del MSPI del MinTIC y la familia de normas ISO/IEC 27000, en sus últimas versiones.
- 7.1.1.2.** Promover la gestión y la seguridad de la información en la FGN.
- 7.1.1.3.** Asegurar la confidencialidad, integridad y disponibilidad de la información generada o bajo custodia de la FGN, almacenada en medios físicos o digitales.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 29 de 111


- 7.1.1.4. Asegurar la continuidad de los servicios que soportan y fortalecen la apropiación del SGSISD.
- 7.1.1.5. Asegurar la continuidad de los servicios y la información generada, que soportan la misionalidad de la entidad.
- 7.1.1.6. Crear, implementar y hacer seguimiento al plan de seguridad y privacidad de la información.
- 7.1.1.7. Crear la documentación (manuales, procedimientos, guías, instructivos, formatos, etc.) y lineamientos (políticas, actos administrativos, etc.), necesarios para la apropiación, desarrollo y cumplimiento del SGSISD.
- 7.1.1.8. Mantener el SGSISD en la FGN.
- 7.1.1.9. Integrar en el SGSISD al Sistema de Gestión Integral SGID.
- 7.1.1.10. Adoptar las buenas prácticas de la norma ISO/IEC 27005 y la guía del MSPI del MinTIC para la gestión de activos e implementar un modelo de gestión y administración de activos de información para la entidad.
- 7.1.1.11. Adoptar las buenas prácticas de la norma ISO/IEC 27005 y la guía para la administración del riesgo y el diseño de controles en entidades públicas, del Departamento Administrativo de la Función Pública (en adelante DAFP), e implementar un modelo de gestión y administración de riesgos de seguridad de la información, integrado al sistema de riesgos de la entidad.
- 7.1.1.12. Diseñar y aprobar un plan de tratamiento de riesgos de seguridad de la información.
- 7.1.1.13. Mantener la mejora continua del SGSISD.

Nota. Los objetivos específicos del SGSISD establecidos en el presente documento, desarrollan, complementan y aterrizan “la Política General de SI de la FGN”, artículo primero de la resolución 4004 del 2013.

7.2. ALCANCE DEL SGSISD

Aplica para todos los procesos y niveles de la entidad; así como para los servidores y funcionarios de la FGN, usuarios internos y externos, judicantes, practicantes, proveedores, contratistas, prestadores de servicios de la entidad ya sean públicos o privados y cualquier otro, que en cumplimiento de sus funciones o de sus obligaciones contractuales tengan acceso de cualquier nivel a los activos de información de la FGN.

Entiéndase por activo todo lo que tenga valor para la entidad y que se encuentre dentro del inventario de activos de información de la Fiscalía, como: hardware (servidores, equipos, tablets, etc.), software (sistemas operativos, aplicaciones,

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 30 de 111

bases de datos, paquetes informáticos, etc.), personas (fiscales, investigadores, servidores, directores, etc.), lugares (archivo permanente, archivo de gestión, bodega de evidencias, etc.), información (manuales, procesos, procedimientos, protocolos, formatos diligenciados, etc.), y cualquier tipo de información física o digital en la que la entidad se encuentre como sujeto obligado por la ley 1581 de 2012, ley 1712 de 2014, decreto 1377 de 2013, o cualquier ley, decreto o norma gubernamental que los reglamente o complemente.

7.3. ROLES Y RESPONSABILIDADES

Los roles y responsabilidades del Modelo de Gestión de SI de la FGN, se definen con el fin de establecer un orden organizacional y jerárquico que disminuya la brecha de error en la implementación del modelo, asegurando que todos conocen y les han sido asignadas y comunicadas sus responsabilidades dentro de la implementación y continuidad de la seguridad de la información de la Entidad.

Los roles y responsabilidades se establecen basados en los requisitos de la norma ISO/IEC 27001:2013 y en los documentos del MSPI del MinTIC: Guía 4 "Roles y Responsabilidades" – 2016, Anexo 1 "Anexo 11.2 Roles y Responsabilidades" – 2021 y el Anexo 4 "Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas" – 2018.

Es así que se cuenta con un modelo que se ajusta a los requisitos de la Fiscalía cuyos sus principales objetivos son: la articulación con todos los niveles de la entidad, áreas, procesos y dependencias necesarios para la implementación, adopción y apropiación del *modelo de seguridad de la información de la FGN*, y monitoreo del desempeño y reporte de seguimiento ante la Mesa Técnica Operativa con funciones de Seguridad de la Información del Comité de Gestión de la Entidad.

Por lo anterior, se establece un modelo jerárquico de roles y responsabilidades para la implementación y continuidad del SGSISD de la FGN.


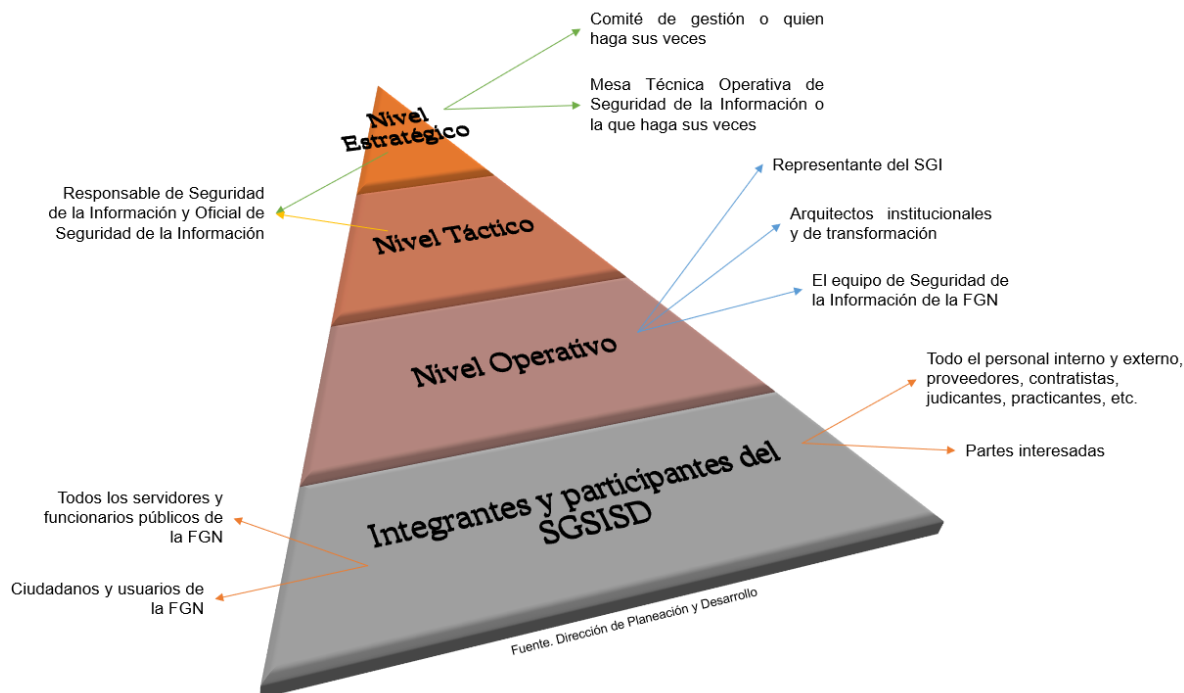
	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 31 de 111

Ilustración 4 Pirámide jerárquica de roles y responsabilidades del SGSISD.




Nota. Los roles y las responsabilidades de Seguridad de la Información y Seguridad Digital fueron adaptados del MSPI del MinTIC a las necesidades de la entidad en alineación con la Arquitectura Institucional, para lo cual los roles de Seguridad de la Información y Seguridad Digital que tengan las mismas funciones o similares dentro de la Arquitectura Institucional, se deberán unir, de tal forma que dichos roles y sus funciones sean ejercidos por un solo cargo, área o grupo.

7.3.1. Mesa Técnica Operativa de Gobierno de Datos, Información y Soluciones Tecnológicas (MTOGD en adelante) perteneciente al Comité de Gestión.

Según las disposiciones del MSPI del MinTIC se requiere que el Comité de Gestión, a través de la MTOGD, gestionen los requerimientos y tareas de SI orientados a:

- Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información, mediante el cumplimiento de las siguientes actividades:
 - Aprobación y seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarios para la implementación interna de las políticas de seguridad y privacidad de la información.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 32 de 111


- Dirigir el plan de toma de conciencia sobre la importancia de adoptar la cultura de seguridad de la información en los procesos, niveles y personal de la entidad.
 - Aprobar acciones y mejores prácticas para la implementación del modelo.
 - Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información.
- Las demás tareas que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad de la información y seguridad digital.
 - Aprobar los planes del SGISD
 - El plan estratégico de seguridad de la información,
 - el plan de continuidad y recuperación de incidentes y desastres, y
 - el plan de tratamiento de riesgos de seguridad de la información.
 - Las tareas que le sean asignadas por el Comité de Gestión en el marco de la SI.

7.3.2. Oficial de Seguridad de la Información

Estará a cargo de liderar la adopción del modelo de seguridad de la información en la FGN; deberá ser creado por acto administrativo y estará vinculado a la planta de la Dirección de Planeación y Desarrollo o de otra área estratégica, pero en ningún caso a la de la Subdirección de TIC (ver lineamiento 7.2.3 *Roles y responsabilidades*, Anexo 1 del MSPI del MinTIC V 4.0).

Será integrante del Comité de Gestión con voz, pero sin voto -artículo 8, Resolución 0-1400 de 2021- y miembro permanente de la MTOGD; las responsabilidades que debería desarrollar según las disposiciones del MSPI del MinTIC para la gestión de los requisitos, la implementación y la adopción del SGSISD y de la SI son:


- Fomentar la implementación de la Política de Gobierno Digital.
- Apoyar en la identificación y aprobación de la política de seguridad de la información y seguridad digital de la Entidad y sus objetivos.
- Definir, elaborar e implementar las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del modelo.
- Proponer la formulación de políticas y lineamientos de seguridad y privacidad de la información.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 33 de 111

- Definir con el responsable de Seguridad de la Información el procedimiento para la Identificación y Valoración de Activos y documentarlo.
- Adoptar el modelo de gestión de riesgos de seguridad de la información y seguridad digital de la entidad y asesorar a la entidad en la identificación e implementación de los controles.
- Apoyar en el Desarrollar el plan de tratamiento de riesgos y su seguimiento.
- Desarrollar en conjunto con el responsable de Seguridad de la Información la Declaración de Aplicabilidad de la Política de Seguridad de la Información.
- Identificar la brecha entre el Modelo de gestión de SI y la situación actual de la entidad (para lo cual se puede usar una de las herramientas ya conocidas como la propuesta por el MSPI del MinTIC).
- Definir e implementar en coordinación con las dependencias de la Entidad, las estrategias de sensibilización y divulgaciones de seguridad y privacidad de la información para servidores públicos y contratistas.
- Poner en conocimiento de las dependencias con competencia funcional, cuando se detecten irregularidades, incidentes o prácticas que atenten contra la seguridad y privacidad de la información de acuerdo con la normativa vigente.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.
- Asesorar y acompañar en conjunto con el responsable de Seguridad de la Información, a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
- Las actividades y responsabilidades asignadas en el marco de la Arquitectura Institucional que se desarrollaran en el manual de AI, basadas en el anexo 1 del MSPI del MinTIC "Anexo 11.2 Guía de Roles y Responsabilidades" – 2021.
- Las que le sean asignadas por la MTOGD o el Comité de Gestión en el marco de la SI.


7.3.3. Responsable de Estrategia de Seguridad de la Información

Estará a cargo de establecer y desarrollar el SGSISD; del diseño del modelo de seguridad de la información de la entidad y de su ciclo de operación. El rol estará vinculado a la planta de personal de la Dirección de Planeación y Desarrollo o de otra área estratégica, pero en ningún caso a la de la Subdirección de TIC (ver lineamiento 7.2.3 *Roles y responsabilidad*, Anexo 1 del MSPI del MinTIC V 4.0).

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 34 de 111

Será miembro MTOGD para los temas de SI cuando se le cite; las responsabilidades que debería desarrollar según las disposiciones del MSPI del MinTIC para la gestión de los requisitos, la implementación y la adopción del SGSISD y de la SI son:

- Asesorar a la Entidad en el diseño, implementación y mantenimiento del Modelo de Seguridad de la Información para la entidad de conformidad con la regulación vigente.
- Crear y desarrollar el documento de implementación del Sistema de Gestión de Seguridad de la Información y Seguridad Digital.
- Definir y gestionar la aprobación de la política de seguridad de la información y seguridad digital de la Entidad y sus objetivos en conjunto con el Oficial de Seguridad.
- Definir, elaborar e implementar las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del modelo.
- Desarrollar la herramienta para la identificación y valoración de los activos información de la entidad.
- Desarrollar el modelo de gestión de riesgos de seguridad de la información y seguridad digital, su entendimiento e implementación en todos los niveles de la entidad (Identificación, Análisis, Evaluación y Tratamiento).
- Desarrollar en conjunto con el Oficial de Seguridad de la Información la Declaración de Aplicabilidad de la Política de Seguridad de la Información.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.
- Realizar la estimación, planificación y cronograma de la implementación del modelo de seguridad de la información adoptado de la Entidad, así como planear las actividades necesarias para una adecuada administración y sostenibilidad de este.
- Liderar la implementación del SGSISD y hacer seguimiento a las tareas y cronograma definido.
- Realizar el acompañamiento a los procesos y /o proyectos en materia de seguridad y privacidad de la información.
- Liderar y brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia.
- Apoyar a los procesos de la Entidad en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 35 de 111

- Definir, socializar e implementar el procedimiento de Gestión de Incidentes de seguridad de la información en la entidad.
- Efectuar acompañamiento a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos en seguridad y privacidad de la información.
- Realizar el acompañamiento a los procesos y /o proyectos en materia de seguridad y privacidad de la información.
- Asesorar y acompañar en conjunto con el Oficial de Seguridad de la Información, a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.

7.3.4. Equipo de Seguridad de la Información de la FGN

Será el equipo de apoyo del Oficial de Seguridad de la Información y del responsable de Seguridad de la Información, se crea por acto administrativo con el fin de apoyar el desarrollo y entregar satisfactoriamente la implementación SGSISD de la Entidad; las responsabilidades y los integrantes que lo conforman están basados en el MSPI del MinTIC.


El personal mínimo que conforme el equipo será:

1. Un profesional responsable de Estrategia de Seguridad de la Información.
2. Profesionales y técnicos en seguridad de la información.
3. Profesionales del SGI.
4. Personal de apoyo.

Se deberá contar con enlaces directos de los procesos de Gestión Jurídica, Control Disciplinario, Control Interno, Mejora Continua, Planeación Estratégica, Gestión de Denuncias y Análisis de la Información e Investigación y Judicialización, los cuales se consultarán dada la necesidad y la etapa de implementación.

Las responsabilidades asignadas son:

- Apoyar al Oficial de Seguridad y al responsable de la Estrategia de Seguridad de la Información al interior de la entidad.
- Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo de la implementación del SGSISD.


	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 36 de 111

- Ayudar al Oficial de Seguridad, en la gestión de proveedores de tecnología e infraestructura.
- Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el Oficial de Seguridad o por el responsable de la Estratégica de Seguridad de la Información.
- Las que considere el responsable de la Estrategia de Seguridad de la Información o la Mesa Técnica de seguridad de la información de la entidad.
- Desarrollar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades necesarias para adoptar el Modelo de Seguridad de la entidad, así como planear las actividades necesarias para una adecuada administración y sostenibilidad de este.

7.3.5. Grupo de Seguridad de la Subdirección de TIC

Grupo perteneciente a la Subdirección de Tecnología de la Información y de las Comunicaciones encargado de vigilar y asegurar la infraestructura tecnología crítica de la Entidad, dentro de sus responsabilidades se encuentra:

- Proponer cambios o actualización de la Política de Seguridad de la información a partir de los riesgos de seguridad identificados en la infraestructura tecnológica crítica identificada en la Entidad.
- Promover la implementación de la Política de Seguridad de la Información adoptada por la entidad.
- Gestionar los lineamientos y estrategias para la actualización y mantenimiento del Sistema de Gestión de Seguridad de la Información y Seguridad Digital (SGSISD) en coordinación con el Oficial de Seguridad de la Información y el Responsable de Seguridad de la Información.
- Contribuir con la formulación e implementación de la Arquitectura de Seguridad Institucional.
- Gestionar pruebas de vulnerabilidades
- Ejecutar la operación de la plataforma tecnológica de seguridad de la información institucional.
- Monitorear los eventos de seguridad ocurridos en la plataforma tecnológica por medio de un SOC.
- Liderar y gestionar los incidentes de seguridad de la información sobre las plataformas propias o tercerizadas.
- Realizar la gestión y el control de los usuarios de la información digital y establecer estrategias de mitigación de riesgos de seguridad de la información garantizando su confidencialidad, integridad y disponibilidad, de acuerdo con los requisitos establecidos.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 37 de 111


Estará conformado por una coordinación y tres equipos de trabajo organizados de la siguiente manera:

- Coordinación de grupo, a cargo de un profesional de la SubTIC que ejercerá como jefe de grupo.
- Equipo de Operación de seguridad de la información
 - Gestión del Centro de Operación de Seguridad SOC:
 - Análisis de primer y segundo nivel.
 - Gestión de Plataformas de seguridad de la información:
 - Gestión de soluciones tecnológicas para la seguridad del dato e intercambio de información.
 - Gestión de plataforma de seguridad perimetral.
 - Gestión de plataforma anti-Malware.
 - Gestión de plataforma SIEM + SOAR.
- Equipo de Gestión de seguridad y privacidad de la información
 - Valoración de arquitectura de seguridad de la información institucional.
 - Implementación de políticas de seguridad de la información.
 - Gestión de concientización de la seguridad de la información a cargo de SubTIC al interior de la entidad.
- Equipo de Investigación y Análisis de seguridad de la información
 - Gestión de riesgos de seguridad de la información en la plataforma tecnológica.
 - Análisis de vulnerabilidades de seguridad.
 - Gestión de conceptos de seguridad.

7.3.6. Propietario o dueño de los activos de información y activos asociados

La FGN define el rol de propietario (dueño) de la información y de los activos asociados, con el fin de garantizar que la información o el activo siempre tenga un dueño o propietario mientras estén relacionados dentro del inventario de activos de información de la Entidad; además define los roles de custodios técnicos y funcionales como complemento a la función que ejerce el propietario (controles A.8.1.2 y A.9.2.5 de la norma ISO/IEC 27001:2013).

Por lo anterior, se establece como propietario o dueño de la información y de los activos de información o activos asociados, al líder del proceso al que éstos pertenecen. En dado caso que, el líder del proceso requiera delegar esta función se

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 38 de 111


podrá hacer a un grupo de trabajo o cargo dentro o fuera de la misma área o proceso; en consecuencia, se puede delegar la función, pero no la responsabilidad, y dicha delegación de funciones se deberá oficializar mediante acto administrativo.

En los casos en que la información o el activo no se encuentre asociada al área en la que el líder del proceso ejerce como superior jerárquico, sino que se encuentra en un área subordinada, el propietario o dueño de la información o del activo será el superior jerárquico de dicha área, quien podrá realizar la delegación de funciones con en las mismas condiciones anteriormente expuestas.

Las responsabilidades del propietario o dueño de la información y de los activos asociados, serán:

- Definir los lineamientos de uso, acceso (restricciones y privilegios), procesamiento, actualización, modificación, borrado y tratamiento de la información y de los activos asociado.
- Tener el conocimiento del proceso o conocimiento del procedimiento involucrado en el proyecto y toma de decisiones sobre aspectos funcionales del sistema de información, de acuerdo con la competencia de su dependencia (área o proceso).
- Validar e informar a la SubTIC, las actividades que requieran los manuales de usuario, según los cambios que se vayan presentado en el aplicativo.
- Coordinar y ejecutar la capacitación funcional de los usuarios del sistema de información, en el nivel nacional, capacidad que adquirirá a partir de la transferencia de conocimientos que le brinde la SubTIC.
- Gestionar las logísticas de la capacitación en el sistema de información, plan de capacitación, generación del material necesario que facilite el entendimiento de los conocimientos del sistema de información.
- Hacer parte en la definición de requerimientos de los aplicativos o sistemas que lidere la SubTIC o el proceso y dar su aprobación a los mismos.
- Hacer seguimiento al cumplimiento de las actividades y responsabilidades de los custodios funcionales.
- Deberá asegurar la implementación, seguimiento y mantenimiento de los controles del anexo A de la ISO/IEC 27001:2013, que se definan para mitigación de los riesgos de SI de los cuales sean responsables (lineamiento de uso, acceso, procesamiento, actualización, modificación, borrado y tratamiento de la información y de los activos asociados).
- Delegar a los custodios funcionales el seguimiento, mantenimiento y cumplimiento de los controles del anexo A de la norma ISO/IEC 27001:2013.

Nota. Para cierto tipo de activos, como son los clasificados como hardware, instalaciones, infraestructura crítica, entre otros tangibles (no se cuentan los intangibles como información, bases de datos y algunos tipos de software y aplicaciones), el custodio técnico también podrá ejercer la

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 39 de 111

función de propietario y custodio funcional, en estos casos la delegación de funciones no se podrá realizar.

7.3.7. Custodios de activos de información y de los activos asociados


Cada activo de información contará con un custodio técnico y uno funcional, encargado de velar por que se cumplan los lineamientos de uso, acceso (restricciones y privilegios), procesamiento, actualización, modificación, borrado y tratamiento de la información y de los activos asociados, dados por el propietario y/o por los propietarios delegados.

7.3.7.1. Custodio Técnico

Cargo o grupo de trabajo de la SubTIC para los activos tecnológicos, cargo o grupo de trabajo de la Subdirección de Bienes para los activos de servicios, instalaciones o comunicaciones, cargo o grupo de trabajo de la Subdirección de Gestión Documental para activos físicos (archivo, papel o digital), cargo o grupo de trabajo de la Dirección de CTI (bodegas de evidencia), para los activos de evidencia de procesos penales. En los casos en los que un área o proceso cuente con herramientas tecnológicas o sistemas de información por fuera de la gobernabilidad de SubTIC, la custodia técnica del activo deberá ser ejercida por un cargo o grupo de trabajo del área o proceso propietario del activo, implementando los controles de SI a que haya lugar conforme a la Política de SI y al manual de implementación del SGSISD de la Entidad.

Por lo cual se establecen las siguientes responsabilidades para los custodios técnicos de SubTIC:

- i) Recibir y custodiar los códigos fuentes, licencias de uso y documentación técnica y de usuario de los sistemas de información a su cargo;
- ii) Participar en la planeación y/o ejecución del diseño, desarrollo, implementación e integración de las soluciones informáticas requeridas por la Entidad que se encuentren en bajo su custodia técnica;
- iii) Elaborar conceptos técnicos sobre la viabilidad de aceptación de las ofertas y productos, en los cuales se determine las posibilidades de sostenimiento como articulación, soporte y transferencia de conocimiento, en el evento que se requiera recibir un ofrecimiento de un sistema de información por parte de un tercero (para SubTIC exclusivamente);
- iv) Coordinar y articular los sistemas de información de la Entidad. Para tal efecto recibirá, consolidará y mantendrá actualizado, el inventario de necesidades en materia de sistemas de información, requerimientos que serán revisados, avalados y priorizados en las sesiones de la MTOGD;

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 40 de 111

Nota. Por requerimiento de la MTOGD se adelantarán sesiones con los respectivos custodios funcionales, delgados por los dueños o propietarios de los activos de información, con el fin de presentar ante la mesa las necesidades, iniciativas y proyectos para su viabilización.

- v) Asegurar la implementación, seguimiento y mantenimiento de los controles del anexo A de la ISO/IEC 27001:2013, que se definan para mitigación de los riesgos de SI de los cuales sean responsables


Los custodios técnicos de los demás tipos de activos mantendrán la seguridad de la información de los activos de información y los activos asociados bajo su custodia, por medio de la implementación, seguimiento y mantenimiento de los controles del Anexo A de la SIO/IEC 27001:2013, que se definan para la migración de los riesgos identificados en los activos y que requieran tratamiento.

Nota. El custodio técnico de los activos de software y centro de computó deberá ser SubTIC. sin embargo, existen dentro de la entidad algunos activos que no han sido desarrollados o adquiridos bajo la supervisión o los lineamientos de SubTIC, por lo que, el presente manual dictará políticas y directrices de SI que controlen los desarrollo o adquisiciones no seguros por fuera de la gobernabilidad de SubTIC, evitando así que queden desarticulados con la Arquitectura Institucional y/o la SI; evitando y previniendo incidentes o eventos que vulneren la integridad, confiabilidad y disponibilidad de la información de la Entidad.

7.3.7.2. Custodio Funcional

Cargo o grupo de trabajo designado por el propietario o propietario delegado del activo, dentro o fuera del área o proceso en donde se encuentra el activo, sus principales funciones son:

- i) Realizar el soporte de primer nivel funcional y procedimental en cuanto a la operación del sistema de información, el manejo y uso de la información, utilizando las herramientas que determine el custodio técnico.
- ii) Participar activamente en las sesiones relacionadas con la definición de requerimientos que lidere el líder técnico.
- iii) Aplicar las pruebas funcionales a los aplicativos que sean desarrollados o adquiridos por la SubTIC o por el proceso, en los ambientes dispuestos.
- iv) Mantener informando al propietario o su delegado, acerca de los resultados de las pruebas funcionales realizadas a los aplicativos desarrolladas o adquiridos.
- v) Deberá asegurar el seguimiento, mantenimiento y cumplimiento de los controles del anexo A de la ISO/IEC 27001:2013, que le sean delegados por el dueño o propietario del activo, siempre y cuando el riesgo asociado

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 41 de 111

se identifique dentro del área en la que se encuentra el custodio funcional.

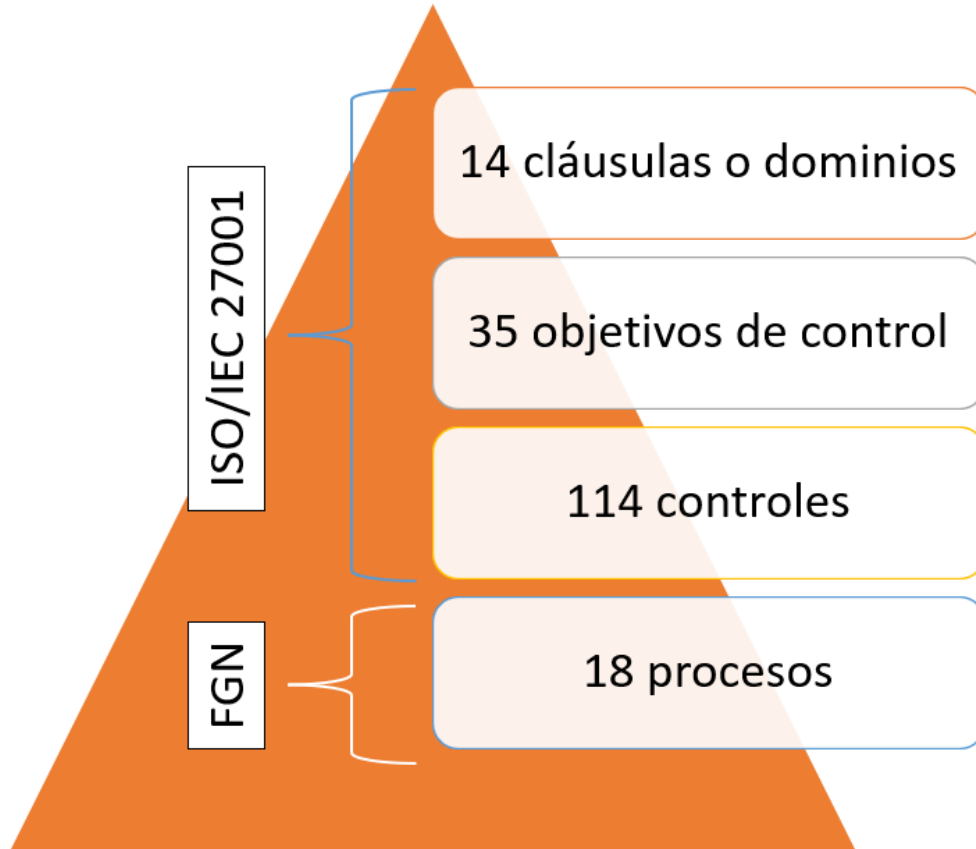
- vi) Para los sistemas de información que así lo requieran, el custodio funcional estará integrado por un grupo de trabajo que garantice la efectiva custodia del activo a través de un líder funcional operativo y uno jurídico.

8. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y DE SEGURIDAD DIGITAL

Como se ve en el numeral 6, el modelo de implementación está basado en la mejora continua; conformado por la Política General de SI, el Sistema de Gestión de Seguridad de la Información y Seguridad Digital -SGSISD- y su manual, las políticas, reglas o lineamientos de seguridad de la información para la Entidad, el inventario de activos de información de la Entidad (por procesos) y el sistema de gestión y administración de riesgos de seguridad de la información, que se desarrollan en un modelo de gestión por procesos.

El Anexo 1 de MSPI del MinTIC, versión 4 del 2021, contempla como marco de referencia la norma ISO/IEC 27001 y su familia de normas; el anexo A de dicho estándar, describe los controles que se deben implementar en una organización para asegurar la disponibilidad, confiabilidad e integridad de la información, además de otros atributos de la seguridad de la información como no-repudio, privacidad legalidad, autenticación y preservación.

Está conformado por 14 cláusulas o dominios, 35 objetivos de control y 114 controles, los cuales deben articularse para su cumplimiento en todos los procesos y áreas de la entidad.




Fuente: Dirección de Planeación y Desarrollo

Modelo del anexo A de la ISO/IEC 27001:2013 con los procesos de la FGN.

La identificación de los controles debe estar documentada y los controles solo se pueden ejercer sobre un activo de información identificado y declarado; haciendo uso de las buenas prácticas, la Fiscalía adopta y adapta a su SGI el modelo de formato⁵⁶ Anexo 1 del MSPI del MinTIC V.4, para la identificación de los controles y como base para la construcción de la batería de controles de seguridad de la información de la FGN.

Por lo anterior, se desarrollan a continuación los lineamientos de cumplimiento del SGSISD en los procesos en general y para cada proceso en particular:

⁵⁶ Anexo 11.1 Controles y objetivos de control, Anexo 1 Modelo de Seguridad y Privacidad de la Información MinTIC.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 43 de 111

8.1. LINEAMIENTOS DE CUMPLIMIENTO PARA LA SEGURIDAD DE LA INFORMACIÓN EN LOS PROCESOS

El SGSISD debe integrarse a todos los procesos de la entidad de forma armónica a través de la identificación de los activos de información y la gestión de los riesgos sobre los mismos. A continuación, se describen los requisitos mínimos a desarrollar, implementar y apropiar por proceso, identificados en el Anexo 1 del presente manual, no queriendo decir esto que una vez realizada a valoración de los riesgos de seguridad de la información, no se puedan contemplar de acuerdo con el activo y su criticidad, el desarrollo o la implementación de algún otro control del anexo A de la ISO/IEC 27001:2013, para lo cual es necesario hacer uso de la guía de implementación de controles ISO/IEC 27002:2015.

8.1.1. Realizar el levantamiento, mantenimiento y actualización la matriz de registro de activos de información de su propiedad, en cumplimiento a la documentación que se estandarice para tal fin, partiendo de la identificación de sus activos primarios y secundarios, como pueden ser:

Activos primarios:

- Procesos y actividades misionales.
- Objetivos estratégicos.
- Información (sin importarte el medio en el que se encuentre o su forma de almacenamiento o custodia): SPOA⁵⁷, SIGOB⁵⁸, todo registro documental en físico o digital, etcétera.


Activos secundarios:

- Hardware (servidores, equipos, tablets, celulares, etc.).
- Software (paquete de datos, sistemas operativos, sistemas de información, aplicaciones, bases de datos, etc.).
- Red (fiscatel, etc.).
- Lugares (archivo central, archivo de gestión, edificios, centro de cómputo, bibliotecas, etc.).
- Personas.

Para la Fiscalía General de la Nación, todo el personal ya sea que esté vinculado directamente o no a la entidad, representa un activo de

⁵⁷ SPOA: Sistema Penal Oral Acusatorio

⁵⁸ SIGOB: Sistema de Información y Gestión para la Gobernabilidad Democrática

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 44 de 111

información, por lo que los procesos no requieren declarar individualmente el recurso humano como activo de información, este activo se encontrará en el proceso de Gestión del Talento Humano, quien implementará los controles requeridos de seguridad de la información; las cavidades de dichos controles, que se extiendan a los procesos, serán de obligatorio cumplimiento.

Nota. Las dependencias, grupos o áreas que estén vinculadas a más de un proceso, deberán mantener control sobre la matriz de registro de activos de información bajo su gobernabilidad ya sean físicos o digitales, sin importar el proceso al que pertenezcan; lo anterior, con el fin de mantener control y seguimiento de los riesgos y los controles de los activos del área, siempre respetando los lineamientos del propietario o responsable del activo de información (líder del proceso o cargo de mayor jerarquía dentro del área si el activo es propio de la misma y no del proceso).

- 8.1.2. Identificar la criticidad de los activos de su propiedad basados en los principios de confidencialidad, integridad y disponibilidad de la información; en donde la confidencialidad se establecerá en el cumplimiento de las leyes de protección de datos personales Ley 1581 de 2012 y de transparencia y acceso a la información Ley 1712 de 2014 (matriz de registro de activos de información).


... “La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.”⁵⁹ ...

- 8.1.3. Todos los activos de información deben tener un propietario, por lo que, a los activos identificados dentro del inventario se les debe asignar un propietario, un custodio funcional y un custodio técnico.

Nota. La gestión de activos de información se desarrollará en documento complementario.

- 8.1.4. El custodio técnico de un activo de información debe pertenecer a la Subdirección de Tecnologías de la Información y de las Comunicaciones, sin embargo, si el activo está por fuera de la gobernabilidad de SubTIC, el custodio técnico será asignado por el propietario de activo y éste puede ser interno (personal de la entidad) o externo. En cualquiera de los dos casos, el proceso será responsable técnica, disciplinaria y penalmente, por cualquier vulneración a la seguridad de la información de la Entidad causada por la gestión de dicho activo, ya que éste no puede ser gestionado por la

⁵⁹ A.8.2.1. Clasificación de la información, anexo A, ISO/IEC 27001:2013

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 45 de 111

dependencia que por ley tiene la responsabilidad de las TIC dentro de la entidad (SubTIC).

En este caso, el proceso debe asegurar que los controles de seguridad de la información que no pueda aplicar SubTIC sobre el activo, serán implementados, controlados y administrados completamente por el proceso o dependencia propietaria.

Nota. Puede haber custodios técnicos que no pertenezcan a SubTIC, sin embargo, deben estar aprobados por SubTIC y ejecutar todos los procedimientos y lineamientos del proceso Gestión TIC, cualquier desviación a la ejecución de éstos, vuelca la responsabilidad de la gestión del activo sobre el proceso o la dependencia propietaria. La aprobación del custodio técnico por SubTIC debe quedar documentada, así como las responsabilidades y obligaciones de cada parte.

- 8.1.5. Los propietarios de los activos deben definir las reglas de uso de estos, los límites de acceso y a quien se les deben dar. De ser necesario, pueden delegar esta función al custodio funcional, pero no la responsabilidad.


... “Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.”⁶⁰ ...

Nota. Al implementar el presente lineamiento, se deben tener en cuenta las aclaraciones que se hacen en las notas del numeral 7.3. *Roles y Responsabilidades*.

- 8.1.6. Una vez realizado el levantamiento de los activos de información y la identificación y valoración de los riesgos sobre los activos críticos, se deberá identificar en el anexo A de la norma ISO/IEC 27001:2013, el o los controles adecuados que lo mitiguen; si se encuentra un mejor o nuevo control que no esté en el anexo A, este se debe documentar y ser aprobado previamente por la Mesa Técnica Operativa de SI o quien haga sus veces.

Nota. En el anexo 1 del presente manual, se encuentra a modo de referencia, la relación de los controles y requisitos de la norma, armonizados a los procesos de la entidad desde el punto de vista de gestión estratégica. Sin embargo, es una guía mínima de implementación, ya que los controles de la norma ISO/IEC 27001:2013, se deben implementar, según aplique, a los riesgos identificados en los activos críticos de cada proceso, aunque estos no estén relacionados entre sí en el anexo 1.


⁶⁰ A.8.1.3. Uso aceptable de activos, anexo A, ISO/IEC 27001:2013

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 46 de 111

- 8.1.7. Identificar los requisitos de ley, estatutarios, reglamentarios y contractuales que apliquen a los sistemas de información y a la información del proceso.
- 8.1.8. Realizar gestión y administración de riesgos de SI, con base en la metodología adoptada por la Entidad.
- 8.1.9. Implementar los indicadores que sean necesarios, para el seguimiento y control de la gestión del SGSISD y de riesgos de SI.
- 8.1.10. Cada vez que se realicen cambios físicos, administrativos o de proceso, se debe realizar una revisión de los riesgos y como estos cambios afectan de manera negativa o positiva los activos de información; se realizarán los respectivos ajustes de gestión de riesgos, para evitar desviaciones que afecten la seguridad de la información.
- 8.1.11. Cada riesgo deberá tener mínimo un indicador por el cual se pueda evaluar el estado del riesgo, y la eficiencia y eficacia de los controles.
- 8.1.12. Los riesgos de los activos que tengan la propiedad compartida entre más de un proceso o área deberán tener mínimo un indicador a cargo del proceso o área propietario, que tenga a cargo el dato fuente del indicador.
- 8.1.13. Apropiar y cumplir la Política General de SI, los objetivos y alcance del sistema y las políticas, reglas o lineamientos de SI.
- 8.1.14. Cumplir los requisitos del presente manual y sus documentos complementarios, según aplique a cada proceso (consultar como referencia anexo 1).
- 8.1.15. Cumplir con los roles y responsabilidades definidos para la SI.
- 8.1.16. Sensibilizar al personal de cada proceso, acerca de los activos de información de su propiedad, la criticidad e importancia de estos y la obligatoriedad de informar sobre violaciones de seguridad de la información que se detecten o conozca.

Para lo anterior, se desarrollarán canales o mecanismos seguros dentro de cada proceso, por medio de los cuales se pueda informar acerca de las posibles violaciones a la seguridad de los activos de información del proceso.

- 8.1.17. Revisar la documentación de los procesos y ajustarla, según aplique, al presente manual y a los documentos del sistema y a los lineamientos, reglas, directrices y políticas que se dicten de la materia. De ser necesario se creará nueva documentación (procedimientos, guías, formatos, etc.), con el fin de dar cumplimiento a la Política General de SI, e implementar y apropiar el SGSISD.

 FISCALÍA <small>GENERAL DE LA NACIÓN</small>	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 47 de 111


La documentación de SI del proceso se debe revisar periódicamente para asegurar que se ajusta y cumple los requisitos de seguridad de la información de la entidad.

... “Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.”⁶¹ ...

Nota. Para la implementación, desarrollo y apropiación del SGSISD, se encuentra como referencia en el anexo 1 de este documento, la relación de los controles y los requisitos de la norma ISO/IEC 27001:2013 con respecto a los procesos del SGI, como guía para la implementación.

- 8.1.18. Cuando hay un empleado nuevo en el área o proceso, ya sea por vinculación, traslado, reasignación de funciones, etcétera, se deberán informar por escrito las obligaciones y responsabilidades asignadas de seguridad de la información para la tarea o trabajo que se va a realizar, hacer firmar acuerdos de confidencialidad si corresponde y remitirlos al área competente para su custodia y almacenamiento.
- 8.1.19. Revisar los derechos de acceso permitidos a los activos de información de su propiedad e información los cambios a Gestión TIC y Gestión Documental.
- 8.1.20. Informar a Gestión TIC y Protección y Asistencia (Departamento de Seguridad), la revocación o asignación de derechos de acceso a los activos de información cuando haya variaciones en las funciones, traslados, encargos, asignaciones, desvinculación, etc.
- 8.1.21. Revisar periódicamente o cuando se cumpla el ciclo de implementación del modelo de seguridad y privacidad de la información de la FGN, los procedimientos y actividades del proceso y asegurar que estén conformes con los requisitos del SGSISD.
- 8.1.22. En caso de materializarle un evento de seguridad de la información, los procesos del SGI de la Entidad deben tener claro los procedimientos y las actividades que se deben ejecutar y/o las autoridades con las que se deben poner en contacto acerca de la violación de la seguridad de la información, estos eventos pueden ser desde desastres naturales, incendios, hasta intrusiones deliberadas informáticas o físicas, etc.

⁶¹ A.18.2.2. Cumplimiento de las políticas y normas de seguridad, anexo A, ISO/IEC 27001:2013


	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 48 de 111

- 8.1.23. A la hora de realizar la gestión de un proyecto, los procesos deben asegurarse de aplicar los lineamientos de seguridad de la información que se definan para la gestión de éstos.
- 8.1.24. Aplicar a los eventos que amenace la seguridad de la información, el procedimiento de acciones disciplinarias, cuando el origen son acciones humanas deliberadas realizadas por personal de la Entidad.
- 8.1.25. Si el evento de seguridad de la información tiene un origen deliberado humano, se debe poner en conocimiento de las autoridades correspondientes o hacer compulsas de copias y asegurar los EMP⁶² para el inicio de la investigación penal.
- 8.1.26. El uso de programas utilitarios y software debe ser autorizada por la SubTIC, por lo que ningún proceso, área, dependencia, servidor o trabajador de la entidad (interno o externo), puede hacer la instalación de este tipo de programas en equipos de la entidad o que estén dentro de la red de la entidad, ya que ponen en riesgo la seguridad de la información.
- 8.1.27. Se deben identificar las áreas (oficinas, archivos, centro de cómputo, salas de recepción de denuncia, etcétera), en las que se almacena, maneja, transforma, procesa o adquiere información crítica, implementar perímetros de seguridad y administrar los riesgos y controles asociados que permitan asegurar la confidencialidad, disponibilidad e integridad de la información.
- 8.1.28. Las reglas para el uso de activos de información, activos críticos o manejo de información fuera de las instalaciones de la entidad deben ser claras en todos los procesos, con el fin de prevenir cualquier vulneración a la seguridad de la información.
- 8.1.29. Los servidores y trabajadores de la entidad deben tomar consciencia de los “equipos con usuario desatendido”, son aquellos equipos que dejan sin supervisión con secciones abiertas, claves de acceso escritas o autocompletables, información confidencial o crítica visible, etc.

Lo anterior no solo aplica para información guardada en medios electrónicos o digitales, también aplica para información física, como son archivos, expedientes, documentación con información confidencial o privilegiada, etcétera; la cual quede, por descuido o negligencia, al alcance de una persona no autorizada para su uso.

- 8.1.30. Los servidores y trabajadores de la entidad, deben tomar consciencia de las posibles afectaciones a la seguridad de la información y su impacto para la entidad, por introducir códigos maliciosos de forma involuntaria o


⁶² EMP: Elemento Material Probatorio

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 49 de 111

accidental, al conectar medios extraíbles infectados como USB u otros, a equipos conectados a la red de la entidad o accediendo a sistemas de información de la FGN desde equipos sin seguridad o que representen una amenaza, como equipos de cafés internet, equipos propios conectados a redes públicas o sin antivirus o sin software licenciado.

- 8.1.31. El personal de la entidad con acceso a activos de información, deben informar cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
- 8.1.32. Antes de llevar a cabo contrataciones con proveedores, los procesos o las dependencias deben identificar los activos de información o las áreas de procesamiento de información crítica a las que tendrán acceso, el nivel de acceso y los permisos de uso que van a tener, etc.; estas responsabilidades, condiciones y obligaciones, se deben comunicar en el proceso contractual para que los oferentes las conozcan y las acepten.
- 8.1.33. Los procesos deberán asegurar que los servicios tercerizados o que sean prestados por terceros (proveedores de servicios o contratistas) a nombre de la entidad apliquen, cumplan y apropien los lineamientos, políticas y directrices de SI establecidas por la FGN, durante todo proceso y las fases de planeación, desarrollo, ejecución y entrega del servicio, así como sobre todos los activos primarios y secundarios (herramientas de TI hardware y software, personal, instalaciones, etc.) que los soporten.
- 8.1.34. Los procesos y áreas deberán adoptar dentro de sus actividades, la documentación transversal para el SGI que otros procesos emitan en cumplimiento de los requisitos de seguridad y privacidad de la información y que les sean aplicables.
- 8.1.35. Los convenios de intercambio de información entre la Fiscalía General de la Nación y otras entidades de estado, se podrán hacer según la clasificación de dicha información así:
- Para la información identificada dentro del ÍCR⁶³ o en la *matriz de registro de activos de información de la FGN*, como “información pública reservada”, “información pública clasificada” o “información pública clasificada y reservada”, solo se podrá hacer el intercambio de información bajo convenio, debidamente firmado por la entidad receptora y la entidad propietaria de la información, quien será la responsable del cumplimiento y los lineamientos de dicho intercambio.

⁶³ ÍCR: Índice de Información Clasificada y Reservada de la FGN.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 50 de 111

- Para la información identificada como “información pública” dentro del registro de información pública de la FGN o la *matriz de registro de activos de información de la FGN*, se podrá hacer intercambio los bajos lineamiento establecidos por la FGN o la documentación del SGI, sin la necesidad de un convenio.

8.1.36. Los servidores, contratistas y empleados de todos los procesos y áreas de la entidad, deben generar conciencia de la confidencialidad que se debe tener con el uso de la información secreta de autenticación e informar y cambiar la información secreta de autenticación siempre que haya un indicio de que se comprometió su seguridad.

... “Mantener la confidencialidad de la información secreta de autenticación, asegurándose de que no sea divulgada a ninguna otra parte, incluidas las personas con autoridad.


Evitar llevar un registro (por ejemplo, en papel, en un archivo de software o en un dispositivo portátil) de la información secreta o de autenticación, a menos de que se pueda almacenar de forma segura y que el método de almacenamiento haya sido aprobado (por ejemplo, una bóveda para contraseñas).⁶⁴...

8.1.37. Los propietarios de la información deben identificar y documentar los requisitos estatutarios y reglamentarios que se deben aplicar a la información generada, obtenida, transformada, controlada o bajo custodia de la entidad y compartirlas con SubTIC para que sean tenidos en cuenta como requisitos de desarrollo en los sistemas de información; además de incluir en éstos, las obligaciones contractuales para los softwares adquiridos y los desarrollados externamente.

8.2. SEGURIDAD DE LA INFORMACIÓN PARA LOS RECURSOS HUMANOS

El proceso Gestión del Talento Humano realiza las actividades de selección, vinculación e ingreso de personal a la Entidad y custodia la información asociada a éste durante su permanecía en la entidad y aún después de su retiro o desvinculación.

⁶⁴ 9.3.1. Uso de información secreta de autenticación, ISO/IEC 27002:2015


	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 51 de 111

Por lo anterior el proceso deberá tener en cuenta los siguientes lineamientos de cumplimiento de seguridad de la información, para los activos propios del proceso, y su activo principal que es el recurso humano de la Entidad:

- 8.2.1. Definir la modalidad de teletrabajo y de trabajo en casa; desarrollar en conjunto con los procesos que aplique, las reglas para la protección de la información en esta modalidad.
- 8.2.2. Verificar que se cuente con todos los requisitos de seguridad de la información para los procesos de selección de personal; ajustar los procedimientos, de ser necesario, para su cumplimiento.
- 8.2.3. Incluir dentro de los procesos de vinculación, de inducción y reinducción al puesto de trabajo, las obligaciones y responsabilidades que se deben en cumplir en cuanto a seguridad de la información.
- 8.2.4. Desarrollar un programa de capacitación, formación y sensibilización acerca de la seguridad de la información para toda la entidad, e incluirlo en el Plan Institucional de Formación y Capacitación PIFC.
- 8.2.5. Definir y comunicar a los servidores, contratistas, judicantes, practicantes, y de más, las responsabilidades y condiciones de seguridad de la información que continúan vigentes después del retiro, desvinculación, traslado, encargo, asignación de funciones, etc.
- 8.2.6. Se debe asegurar que dentro del paz y salvo por traslado, desvinculación, retiro o cualquier otro movimiento de personal que involucre el cambio de funciones o responsabilidades, se haga entrega de los activos de información que se tenían a cargo y se revoquen o cambien los accesos permitidos.
- 8.2.7. Los procedimientos de desvinculación o traslados deben asegurar la terminación de los privilegios de acceso a la información, sistemas e instalaciones y dependencias a los que ya no se debe tener acceso.
- 8.2.8. Desarrollar programa de motivación o incentivos para los servidores que haya tenido acciones destacadas para la protección de la seguridad de la información de la entidad.

8.3. SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE TECNOLOGÍAS DE LAS INFORMACIÓN Y LAS COMUNICACIONES

La seguridad de la información en la gestión de activos involucra los procesos que tienen a su cargo la custodia técnica de activos de información, como son Gestión Documental, Gestión TIC e Investigación y Judicialización para las bodegas de evidencia.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 52 de 111

En cuanto a las tecnologías de la información y las comunicaciones, según el decreto Ley 016 de 2014, artículo 39, literal 2 ... *“Liderar, coordinar y monitorear la plataforma de tecnologías de la información y la comunicación de la Fiscalía General de la Nación, que apoye el cumplimiento de sus funciones.”*..., literal 3 ... *“Liderar, coordinar y articular los diferentes sistemas de información de la entidad.”*..., y el literal 9 ... *“Gestionar, atender, proponer e implementar las políticas y acciones relativas a la seguridad y oficialidad de la información y de la plataforma tecnológica de la Fiscalía General de la Nación.”*..., es la Subdirección de Tecnologías de la

Información y de las Comunicaciones, a través del proceso de Gestión TIC, es la que tiene la función de ejercer la custodia técnica de los activos de *infraestructura tecnológica y de comunicaciones*⁶⁵ de la entidad, por lo que en el marco de SGSISD deberá:


- 8.3.1. Desarrollar, implementar y revisar en conjunto con el proceso de planeación estratégica, la Política General de SI.
- 8.3.2. Desarrollar, implementar y revisar, las políticas y directrices de seguridad de la información propiedad del proceso de Gestión TIC, como se muestra en el anexo 2.
- 8.3.3. Construir en conjunto con mejora continua y planeación estratégica, el esquema de roles y responsabilidad de seguridad de la información de la entidad, teniendo en cuenta la segregación de funciones.
- 8.3.4. Desarrollar en conjunto con el proceso de planeación estratégica y mejora continua, los procedimientos para identificar y reportar los incidentes de seguridad de la información; teniendo en cuenta que actividades se deberán desarrollar y a que autoridades se deberá informar.

Nota. En cumplimiento de la resolución del 1519 del 2020 emitida por el MinTIC, dentro del presente lineamiento se deben desarrollar y estandarizar aquellas actividades que permitan identificar, gestionar y dar trámite de los incidentes de ciberseguridad en el interior de la Entidad y su comunicación con el CSIRT⁶⁶ y/o ColCERT⁶⁷.

⁶⁵ Los activos de infraestructura tecnológica y de comunicación, son todos aquellos que interfieren y gestionan los procesos informativos y de comunicación, como son: hardware, software, telecomunicaciones, automatización y comunicación de negocios y servicios de TI, entre otros.

⁶⁶ CSIRT (ver definiciones y siglas). Según el Decreto 338 de 2022, artículo 2.2.21.1.5.1. ... *“Los equipos de respuestas a incidentes de seguridad digital son: [...], el CSIRT - Gobierno - Equipo de Respuesta a Incidentes de Seguridad digital de Gobierno, CSIRT - Defensa - Equipo de Respuesta a Incidentes de Seguridad digital del sector Defensa, el CSIRT del Sector Inteligencia” los CSIRT - Sectoriales - Equipos de Respuesta a Incidentes de Seguridad digital de los sectores definidos como críticos o prestadores de servicios esenciales.”* ... Para la atención y gestión de incidentes de seguridad digital el COLCERT - Equipo de Respuesta a Emergencias Cibernéticas de Colombia


⁶⁷ COLCERT ver definiciones y siglas). Según el Decreto 338 de 2022, artículo 2.2.21.1.5.1. ... *“Los equipos de respuestas a incidentes de seguridad digital son: Para la atención y gestión de incidentes de seguridad digital el COLCERT - Equipo de Respuesta a Emergencias Cibernéticas de Colombia, [...]”* ...

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 53 de 111

- 8.3.5. Mantener contacto con grupos de interés para mantenerse actualizado en requisitos, mejores prácticas, comprensión del entorno, advertencias tempranas de ataques y vulnerabilidades, etc.
- 8.3.6. Establecer los requisitos para los acuerdos contractuales en cuanto a la propiedad intelectual, así como los derechos legales dentro del desarrollo de software y las responsabilidades de contratistas y empleados referentes a seguridad de la información.
- 8.3.7. Exigir a los contratistas el cumplimiento de los lineamientos de seguridad de la información y controlarlo.
- 8.3.8. Aplicar los controles aprobados a los activos de información digitales que se encuentren identificados dentro del inventario de activos de información y sobre los que ejerza función como propietario, custodio técnico o custodio funcional.

Nota. La SubTIC no tendrá responsabilidad de implementar controles sobre activos informáticos y de comunicaciones que no estén declarados en el inventario de activos de información como custodio técnico, esto es: desarrollos de software, aplicaciones o servicios, red, hardware, software, convenios de intercambio de información, etc., los que hayan sido desarrollados por los procesos sin contar con la SubTIC y por fuera de la Arquitectura Institucional. En estos casos se aplicarán los lineamientos 8.1.4 y 8.1.26.


- 8.3.9. Se deberá implementar dentro del SGSISD lineamientos, procedimientos, actividades documentadas, sistemas o herramientas, entre otros, para:
 - a. La gestión de medios removibles, su disposición y transferencia.
 - b. El registro y cancelación de registro de usuario que permitan también, la asignación de derechos de acceso.
 - c. Asignación y revocación de derechos de acceso otorgados a las identificaciones de los usuarios, para todo tipo de usuarios y para todos los sistemas y servicios.
 - d. Restringir y controlar la asignación y uso de derechos de acceso privilegiado asociados a cada sistema o proceso, conforme a la política de control de acceso.
 - e. Cancelación de los derechos de acceso a usuario que hayan terminado el empleo con la entidad, desvinculación o finalización del contrato, o revocar, revisar y reasignar los derechos de acceso para los que hayan cambiado de funciones, ascenso, traslado, encargo, asignación, etc., en concordancia con 8.1.19, 8.1.20, 8.2.6 y 8.2.7.
 - f. Asignación formal de información secreta de autenticación, para asegurar que se conozcan las responsabilidades, deberes y prohibiciones en el uso de la información de autenticación secreta, así como los privilegios de uso

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 54 de 111

otorgados para la información y los activos de información, teniendo en cuenta su nivel de criticidad y sensibilidad.

- g. Restringir el acceso a la información y a las funcionalidades de las aplicaciones, conforme a la política de control de acceso y los requisitos de la entidad.
 - h. En los casos que se requiera, adoptar una técnica de autenticación para corroborar la identidad declarada del usuario.
 - i. Asegurar que se cumple con la guía de implementación ISO/IEC 27002:2015 numeral 9.4.3, en la implementación del sistema de gestión de contraseñas.
 - j. Controlar y restringir el uso de programas utilitarios privilegiados en la entidad por fuera de la SubTIC.
 - k. Prohibir, controlar y restringir el acceso a los códigos fuentes de los programas.
... “Se debería controlar estrictamente el acceso a los códigos fuente de los programas y elementos asociados (tales como diseños, especificaciones, planes de verificación y planes de validación), con el fin de evitar la introducción de funcionalidad no autorizada y para evitar cambios involuntarios y mantener la confidencialidad de la propiedad intelectual valiosa.”⁶⁸ ...
 - l. Disponer de los medios tecnológicos, controles y protocolos de seguridad y comunicaciones, entre otros, para el desarrollo de convenios de intercambio de información de la Fiscalía General de la Nación con otras entidades.
- 8.3.10. Desarrollar, implementar y gestionar en conjunto con Mejora Continua y Gestión Documental, el inventario de activos de información de la entidad, que abarque el ciclo de vida de la información (creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción).
- 8.3.11. Identificar y documentar las actividades que constituyen una violación a la seguridad de la información de la entidad.
- 8.3.12. Identificar y proteger las áreas de tengan, manejen o procesen información crítica o sensible de la entidad, conforme a los requisitos de seguridad de los activos dentro del perímetro y la valoración de riesgos.
- 8.3.13. Asegurar que las áreas identificadas (8.3.12) se protegen para controlar el acceso de personal no autorizado conforme a la criticidad y a la sensibilidad de la información y la valoración de los riesgos.
- 8.3.14. Velar por que se mantengan activos y en funcionamiento los servicios de suministro de electricidad, comunicaciones, agua, gas, alcantarillado,

⁶⁸ 9.4.5. Control de acceso a códigos fuente de programa, ISO/IEC 27002:2015

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 55 de 111


ventilación y aire acondicionado, entre otros, para los equipos de su gobernabilidad.

8.3.15. Desarrollar e implementar individualmente o en conjunto con otros procesos (cuando así lo exija el mantener la seguridad de la información), procedimientos o actividades documentadas, herramientas, sistemas, etc.:


- a. Las mejores prácticas para asegurar que las líneas de energía eléctrica y de telecomunicaciones que portan datos o brindan soporte a los servicios de información, estén protegidas contra interceptación, interferencia o daño.
- b. Procedimientos que mantengan en óptimas condiciones los equipos que soportar los servicios de telecomunicaciones y de información, y que aseguren la continuidad de la disponibilidad e integridad de la información.
- c. Lineamientos para prevenir que los equipos, la información o los activos sean retirados de su sitio seguro por personal sin autorización, para lo cual los procesos y los propietarios de los activos definirán quienes, en qué tipo de actividades y por cuánto tiempo se autoriza el retiro del sitio seguro.
- d. Herramientas y procedimientos que aseguren que los equipos de almacenamiento o procesamiento de información o la información, no va a sufrir incidentes de seguridad, cuando éstos son retirados de las instalaciones de la entidad o de su sitio seguro, basándose en la valoración de los riesgos de los activos de información.
- e. Asegurar que los equipos dañados o dispuestos para dar de bajar no contengan información crítica o sensible, se deben evaluar los riesgos y las opciones para evitar la extracción de dicha información, se podrían contemplar soluciones como destruir la información, eliminarla o sobre escribirla, en cualquier caso, se debe contemplar la destrucción física del equipo si existe riesgos de recuperación.
- f. Implementar herramientas para dar seguridad a los equipos de usuarios desatendidos mediante mecanismos de bloqueo de pantalla, Log-Off de las aplicaciones o servicios de red, etc.

8.3.16. Desarrollar o revisar las actividades de operación para las instalaciones de procesamiento y comunicación y asegurar que estén documentadas y actualizadas en lo referente a:

- a. Encendido y apagado de equipos,
- b. mantenimiento de equipos,
- c. manejo de medios,


	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 56 de 111

- d. salas de cómputo,
 - e. gestión y seguridad del manejo de correo,
 - f. instalación y configuración de sistemas,
 - g. procesamiento y manejo de información (manual y automático),
 - h. copias de respaldo (desarrollado en conjunto con la política de copias de respaldo),
 - i. requisitos de programación e interdependencias con otros sistemas y tiempo de finalización de primer y último trabajo,
 - j. instructivo de manejo de errores y otras situaciones excepcionales con las restricciones sobre uso de utilidades del sistema,
 - k. en caso de dificultades técnicas u operaciones, definir escalamientos y contactos de soporte externo,
 - l. disposición segura de elementos de salida de trabajo fallido,
 - m. procedimientos de reinicio y recuperación de sistema,
 - n. gestión de rastros de auditoría (audit trail) y de información de registros de sistema (system log) y,
 - o. procedimientos de seguimiento.
- 8.3.17. Gestionar y documentar los cambios significativos en los procesos misionales o aquellos que afecten o modifiquen la estructura de TIC de la entidad, se deben contemplar:
- a. Los cambios significativos,
 - b. planificar y poner a prueba dichos cambios,
 - c. valorar el impacto de los riesgos que provocan los cambios,
 - d. tener procedimientos de aprobación formal de los cambios,
 - e. revisión de los requisitos de seguridad de la información,
 - f. informar de los cambios a los propietarios o interesados,
 - g. actividades de apoyo, procedimientos y responsabilidades para cambios no exitosos, recuperarse de ellos y eventos no previstos y,
 - h. procesos de cambio de emergencia para recuperarse rápidamente de un incidente.
- 8.3.18. Evaluar la capacidad presente y futura de los sistemas críticos para la entidad, con base en los requisitos de crecimiento esperados y a la disponibilidad y eficiencia requerida para éstos.
- 8.3.19. Separar los ambientes de desarrollo, prueba y producción y evitar cambios y accesos no autorizados, en alineación con la política de desarrollo seguro.
- 8.3.20. Desarrollo de lineamientos de toma de conciencia para el personal de TIC y de la entidad, con el fin proteger contra códigos maliciosos; además de


	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 57 de 111

implementar una herramienta de detección y reparación, y medir la eficacia y la eficiencia de las acciones tomadas.

- 8.3.21. Elaborar, conservar y hacer seguimiento y control de los registros de eventos de usuarios, excepciones, fallas y eventos de seguridad de la información; estos registros deben contener todas las posibles variables que arroje cada sistema para controlar y conservar evidencia de estos, además de:
- a. Los administradores de sistema no deberían tener permisos para desactivar o borrar los registros (logs) de sus actividades.
 - b. Implementar herramientas o controles para proteger contra cambios no autorizados la información de registro, contra problemas operacionales en los sistemas de control de registros (como alteraciones en los tipos de mensaje, archivos de registro editados o eliminamos, sobre escritura de los registros y capacidad insuficiente de almacenamiento).
 - c. Proteger y revisar los registros (Logs) para mantener la rendición de cuentas de usuarios privilegiados y así prevenir la manipulación de los Logs.
 - d. Sincronización con la hora legal de Colombia de todos los dispositivos que se conecte a la red de la entidad.
- 8.3.22. Controlar la instalación de software en sistemas operativos. Debe ser privilegio de SubTIC la instalación o la autorización de instalación de software operacional, aplicaciones y librerías de programas.
- 8.3.23. Realizar gestión eficaz de vulnerabilidades técnicas sobre los activos de información declarados en el inventario del proceso y sobre los que actúa como custodio técnico, en cumplimiento a la *política de prohibición de uso e instalación de software no autorizado*.
- 8.3.24. Desarrollar actividades documentadas que prevengan, controlen y minimicen la interrupción de sistemas operativos por auditorías de verificación, ventanas de mantenimiento y salidas de operación no programada, entre otras, que excedan el tiempo de indisponibilidad tolerable.
- 8.3.25. Implementar herramientas o procedimientos para gestionar la seguridad de las redes:
- a. Controlar la seguridad de la información en las redes y la protección de servicios relacionados, contra accesos no autorizados.
 - b. Identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de los servicios de red, para ser incluidos en los acuerdos de servicio de red.


	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 58 de 111

- c. Realizar seguimiento al proveedor de servicios de red para asegurar la prestación de los servicios acordados, evaluar la pertinencia de acordar contractualmente los derechos de auditoría.
 - d. Identificar los acuerdos de seguridad necesarios para los servicios particulares, tales como características de seguridad, niveles de servicio, requisitos de gestión, etc.
 - e. Dividir las redes en dominios de red separados como método para gestionar la seguridad de la red.
- 8.3.26. Establecer actividades documentadas para asegurar que la seguridad de los sistemas de información está durante todo su ciclo de vida, teniendo en cuenta que:
- a. Establecer los requisitos de seguridad de la información para nuevos desarrollos y para mejoras de los existentes, conforme al tipo de información del activo y su criticidad; para esto, se pueden usar métodos como, por ejemplo, obtención de requisitos de cumplimiento a partir de políticas y reglamentación, modelado de amenazas, revisión de incidentes, umbrales de vulnerabilidad, entre otras buenas prácticas.
 - b. Proteger de actividades fraudulentas, divulgación y modificación no autorizada, la información de los servicios y aplicaciones que pasa sobre redes públicas, si los hay.
 - c. Proteger la información que hace parte de las transacciones de los servicios de las aplicaciones, contra transmisión incompleta, enrutamiento errado, alteración no autorizada de mensaje, divulgación no autorizada, duplicidad y reproducción de mensaje no autorizado.
- 8.3.27. Dentro del proceso de desarrollo de software, se deben considerar procedimientos de control de cambios documentados para asegurar la integridad del sistema.
- 8.3.28. El desarrollo de nuevos sistemas o aplicaciones, o cambios a los sistemas existentes, deben tener un proceso de documentación, especificación, pruebas, control de calidad, gestión de la implementación y valoración de riesgos, análisis de los impactos de los cambios y especificación de los controles de seguridad necesarios.
- 8.3.29. Ante cambios en la plataforma de operación se deben revisar las aplicaciones críticas de negocio y someterlas a pruebas, asegurándose de que no haya impactos adversos que afecten la seguridad de la información. Revisar los procedimientos de integridad y control de las aplicaciones y ajustar los planes de continuidad de negocio.
- 8.3.30. En los casos de modificaciones de los paquetes de software, se deben evaluar los riesgos de integridad de los procesos y la afectación de los

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 59 de 111


controles que conlleva, tanto en desarrollo internos como externos. Cuando sean software adquiridos, los cambios y actualizaciones se deben obtener del vendedor.

- 8.3.31. Implementar procedimientos documentados, para establecer y mantener los principios de construcción de software seguro, que sea aplicable a cualquier implementación de sistemas de información, e incluir todas las capas de arquitectura para el diseño, negocio, datos, aplicaciones y tecnología.
- 8.3.32. Establecer y proteger el ambiente de desarrollo haciéndolo seguro durante todo el ciclo de vida del desarrollo de sistemas, incluyendo a las personas, procesos y tecnología asociados en el desarrollo e integración de sistemas.
- 8.3.33. Definir procedimiento de pruebas y validaciones completas, durante los procesos de desarrollo en los sistemas nuevos y las actualizaciones, incluido el programa detallado de actividades y entrada de las pruebas y salidas esperadas. Llevar a cabo pruebas de aceptación independiente para los desarrollos internos como para los contratados externamente.
- 8.3.34. Establecer programas de prueba para la aceptación de los sistemas de información nuevos, actualizaciones y nuevas versiones, en donde entre los criterios de aceptación se deben tener en cuenta los requisitos de seguridad e la información y la adherencia a las prácticas de desarrollo seguro establecidas; entre otros, e incluir todas las posibilidades de nuevos sistemas e integraciones.
- 8.3.35. Proteger y controlar los datos que se usen para pruebas en los desarrollos, éstos se deben seleccionar de los datos operacionales eliminando o cambiando los datos personales o cualquier información confidencial, siendo cuidadosos del cumplimiento de la ley de protección de datos personales.
- 8.3.36. Dentro de los acuerdos con los proveedores que se establezcan en cumplimiento a la *política de seguridad de la información en relación con los proveedores*, se deben tener claros los compromisos de seguridad de la información entre ambas partes y los requisitos para tratar los riesgos asociados a los servicios de TIC.
- 8.3.37. Definir lineamientos de seguimiento y revisión de la prestación de servicios de los proveedores de TIC, en el cumplimiento de los términos y condiciones de seguridad de la información y las aprobaciones de los cambios en el suministro del servicio, mantenimiento, mejora de las políticas, procedimientos y controles de seguridad teniendo en cuenta la criticidad de

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 60 de 111

la información, sistemas y procesos de negocio involucrados y revaloración de los riesgos.

- 8.3.38. Se deben determinar procedimientos, canales y responsabilidades para la gestión eficiente de incidentes de seguridad de la información de TIC, esto en concordancia con los lineamientos que se establezcan desde Mejora Continua.
- 8.3.39. Establecer, implementar y mantener un sistema documentado de continuidad de seguridad de la información para prepararse, mitigar y responder ante situaciones y eventos adversos, que contemple:
- a. Requisitos de seguridad de la información, continuidad de la gestión de seguridad de la información en circunstancias adversas como crisis o desastre, y gestión para la recuperación de desastres.
 - b. Asignación de responsabilidades y personal con experiencia y competencia.
 - c. Desarrollo de simulacros, pruebas y análisis de los resultados en evento de desastre, crisis o ante un evento perturbador, que ponga a prueba a efectividad de los planes de continuidad de negocio y de recuperación de desastre.
- 8.3.40. Identificar los requisitos de la entidad para la disponibilidad de los sistemas de información con el fin de garantizar su disponibilidad, usando la arquitectura de los sistemas existentes, otros componentes o arquitecturas redundantes.
- 8.3.41. Tener dentro de los requisitos de desarrollo las obligaciones estatutarias, reglamentarias y contractuales de la información, los cuales deben ser entregados por los procesos o áreas propietarios.
- 8.3.42. Establecer y desarrollar las actividades para asegurar que los registros que queden de las transacciones de la información como por ejemplo, registros financieros, registros de bases de datos, registros de transacciones (logs), registros de auditoría de sistemas (Audit logs) y procedimientos operacionales, se protejan contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, basando su nivel de protección en los requisitos y necesidades de la entidad, cada uno con el detalle de los periodos de retención y tipo de medio de almacenamiento como papel, microfichas, medios magnéticos, medios ópticos, llaves criptográficas, etc. Esta tarea se debe llevar a cabo en conjunto con los procesos de Gestión Documental, Mejora Continua e Investigación y Judicialización para las bodegas de evidencia.
- 8.3.43. Desarrollar, documentar e implementar un programa de seguimiento y revisión de los sistemas de información que vigile y controle el cumplimiento de las políticas, directrices y lineamientos del SGSISD.


	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 61 de 111

- 8.3.44. Incluir e implementar los controles para el desarrollo de sitios web y aplicaciones, establecidos por el MinTIC en el numeral 3.2. “Condiciones de seguridad Digital”, del Anexo 3 “Condiciones mínimas técnicas y de seguridad digital” de su resolución 1519 del 2020.
- 8.3.45. Incluir, desarrollar e implementar dentro de los controles de desarrollo seguro, el numeral 3.3. “Programación del código fuente”, del Anexo 3 “Condiciones mínimas técnicas y de seguridad digital” de su resolución 1519 del 2020.

8.4. SEGURIDAD DE LA INFORMACIÓN EN LOS ACTIVOS FÍSICOS

El proceso de Gestión Documental actúa como custodio técnico de los activos físicos, siendo el garante de la seguridad de la información almacenada en sus archivos; comparte esta responsabilidad con los demás procesos en cuanto a que no toda la información física está bajo su custodia, asume solamente esta responsabilidad cuando le es transferida por los procesos, sin embargo, debe impartir lineamientos que aseguren y controlen la seguridad de la información cuando aún está bajo custodia del propietario o de quien la genere.

- 8.4.1. Desarrollar, implementar y revisar, las políticas y directrices de seguridad de la información propiedad del proceso de Gestión Documental, como se muestra en el anexo 2.
- 8.4.2. Identificar los activos de información bajo su custodia técnica y las instalaciones de procesamiento y almacenamiento de información.
- 8.4.3. Identificar el propietario de la información asociada a los activos bajo su custodia y definir roles y responsabilidades de cada parte, estos pueden ser del mismo proceso o de otro.
- 8.4.4. Definir, implementar y documentar las reglas para el uso de la información asociada a los activos bajo su custodia, asegurarse que se cuenta con un esquema adecuado de clasificación y protección según el medio en el que se encuentre, y tener un método apropiado de manejo de los activos cuando es eliminado, transferido o destruido.
- 8.4.5. Desarrollar y documentar en conjunto con mejora continua, un esquema de etiquetado de la información y de los activos de información que incluya los formatos físicos y electrónicos de almacenamiento, y que permita identificar el área y proceso al que pertenecen y el tipo de activo.


	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 62 de 111

- 8.4.6. Desarrollar actividades documentadas para el manejo, procesamiento, almacenamiento y comunicación de la información de conformidad con su clasificación.⁶⁹
- 8.4.7. Definir lineamientos para la gestión, disposición, transferencias de medios removibles físicos dependiendo del ciclo de vida, el tipo y el medio de almacenamiento de la información.
- 8.4.8. Identificar las áreas de almacenamiento y procesamiento de información e implementar:
- a. Perímetros de seguridad,
 - b. controles de acceso físico,
 - c. lineamientos de autorización de ingreso,
 - d. manejo de elementos, medios y de información.

La ubicación y fortaleza de los perímetros de seguridad, así como los demás controles, deberán depender del tipo de información que se encuentra allí, del resultado de la identificación y valoración de los riesgos, de su criticidad y sensibilidad, y de la importancia que tenga para la entidad.

- 8.4.9. Desarrollar e implementar actividades o lineamientos para la protección de los equipos de manejo de información y las áreas de almacenamiento de información, con el fin de proteger contra amenazas de seguridad de la información.
- 8.4.10. Identificar los servicios necesarios en las áreas de manejo y almacenamiento de información como son: electricidad, telecomunicaciones, suministros de agua, etc., ventilación, aire acondicionado, entre otros, y protegerlos contra fallas y otras interrupciones que puedan afectar la disponibilidad o integridad de la información allí almacenada.
- 8.4.11. Se deberán desarrollar lineamientos o reglas para proteger la información cuando ésta es extraída de su lugar de almacenamiento, identificar quienes son los autorizados y sus deberes y responsabilidades en el manejo de la información.
- 8.4.12. Implementar un canal de acceso para la recepción de información anónima o formal, interna o externa, sobre posibles violaciones, incidentes o eventos de seguridad de la información y alinear su respuesta a las actividades que se implementen y documenten para la atención de estos eventos.
- 8.4.13. Establecer en conjunto y documentar, el plan de continuidad de gestión de seguridad de la información, los controles, los requisitos de SI y

⁶⁹ Guía de implementación, numeral 8.2.3, ISO/IEC 27002:2015.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 63 de 111

los requisitos de la continuidad de la gestión en situaciones adversas como crisis y desastres.

- 8.4.14. Revisar periódicamente o cuando hallan cambios significativos de proceso o de procedimientos, de ley, u organizacionales (organigrama, infraestructura física, ubicación, etc.), los controles de seguridad de la información y de continuidad de la gestión seguridad de la información ante situaciones adversas, y asegurar que este si cumplen el propósito de mantener la SI basados en la identificación y valoración de los riesgos y la criticidad y sensibilidad de la información.
- 8.4.15. Mantener actualizado el listado de requisitos legales, reglamentarios y contractuales aplicables a la información del proceso, y tener presentes y bajo control el cumplimiento de los que sean aplicables para la información bajo su custodia (el listado de requisitos, lo deberá suministrar el área o proceso propietario de la información).
- 8.4.16. Aplicar en lo que corresponda para la información en activos físicos el control de protección de registros.


... *“Los registros se deberán proteger contra pérdida, destrucción, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de la entidad.⁷⁰” ...*

8.5. MEJORA CONTINUA EN LA SEGURIDAD DE LA INFORMACIÓN

El proceso de Mejora Continua tiene a cargo apoyar a los procesos de Planeación Estratégica y Gestión TIC, en el establecimiento y la implementación del SGSISD y sus componentes desde el SGI, por lo que, como elementos mínimos a desarrollar en conjunto, se tiene:

- 8.5.1. Revisar y evaluar la pertinencia y el cumplimiento del SGSISD cada vez que se cumpla el ciclo de implementación o cuando sea requerido por la alta Dirección.
- 8.5.2. Desarrollar, documentar e implementar la metodología para la administración y gestión de los riesgos de seguridad de la información y seguridad digital de la FGN.
- 8.5.3. Hacer revisión de cumplimiento al SGSISD cuando se cumpla el ciclo de implementación y realizar revisiones periódicas programadas a los procesos,

⁷⁰ Control A18.1.3. Protección de Registros, ISO/IEC 27001:2013 y numeral 18.1.3. Protección de registros ISO/IEC 27002:2015 (guía de implementación).


	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 64 de 111

para prevenir las desviaciones y asegurar un adecuado desarrollo del sistema.

8.6. PLANEACIÓN ESTRATÉGICA DE LA SEGURIDAD DE LA INFORMACIÓN

La planeación estratégica como representación de la dirección de la Entidad, desarrolla dentro de su proceso el SGSISD, creando y estableciendo dentro del SGI y el esquema normativo de la FGN políticas, lineamientos, directrices, documentos, planes, proyectos y programas de seguridad de la información y seguridad digital, en cumplimiento de la Política General de SI de la FGN, y el MGSI y su ciclo de operación adoptados por la entidad a través del presente manual.

- 8.6.1. En conjunto con los procesos de Gestión TIC y Gestión Documental, realizarán la revisión, actualización y aprobación de la Política General de SI, MGSI, el ciclo de operación del MGSI y el esquema de roles y responsabilidades del SGSISD, basándose en las políticas y directrices adoptadas por la entidad (consultar como referencia anexo 1.2.) y en alineación con la Arquitectura Institucional.
- 8.6.2. Definir las responsabilidades para la protección de los activos de manera individual y los datos de los activos críticos.
- 8.6.3. Incluirá dentro del plan estratégico de la entidad, las metas requeridas para la implementación y continuidad del SGSISD.
- 8.6.4. Gestionar la inclusión dentro de los proyectos de inversión de la entidad, lo necesario para la implementación y continuidad el SGSISD.
- 8.6.5. Construir en conjunto la Política General de SI, gestionar su aprobación, promover su apropiación, y hacer la revisión y ajuste de esta cada vez que se cumpla el ciclo de operación del MGSI de la entidad o cuando haya cambios es los estándares que lo soportan (normas ISO/IEC 27000 y MSPI del MinTIC).
- 8.6.6. Desarrollar, implementar y revisar las políticas y directrices de seguridad de la información de su propiedad, como se muestra en el anexo 2.
- 8.6.7. Construir en conjunto el esquema de roles y responsabilidad de seguridad de la información de la entidad, teniendo en cuenta la segregación de funciones.
- 8.6.8. Aportar en el desarrollo de las políticas, directrices, lineamientos y controles del SGSISD en que se tenga injerencia (ver anexo 2).
- 8.6.9. Desarrollar los procedimientos para identificar y reportar los incidentes de seguridad de la información, que actividades se deberán desarrollar y a que autoridades informar.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 65 de 111

8.6.10. Integrar la seguridad de la información a los métodos de gestión de proyectos desarrollados para la entidad, asegurando que los riesgos de seguridad de la información se identifiquen y se traten de forma temprana. Se debe trabajar la seguridad de la información como un objetivo dentro del proyecto sin importar la naturaleza de éste, y hará parte de todas las etapas de la metodología.

8.6.11. Desarrollar y documentar la metodología para el levantamiento del inventario de activos de información de la entidad, que contenga los aspectos de identificación de propietario, uso y devolución del activo, así como la clasificación, etiquetado y manejo, de la información durante todo su ciclo de vida.

Nota. Las bodegas de evidencia se deberán acogerá a la metodología para la clasificación de los activos de información que adopte la entidad sin perjuicio del Manual de Cadena de Custodia.

8.6.12. Desarrollar el modelo de gobierno de datos de la Entidad y la metodología para su ejecución y apropiación por todos los niveles, áreas y procesos de la entidad.


8.6.13. Desarrollar con el apoyo de Gestión TIC y en conjunto con los procesos de Gestión del Talento Humano y Comunicación y Relacionamento Institucional, el plan de capacitación de toma de conciencia, apropiación, difusión y divulgación del SGSISD de la FGN.

8.6.14. Desarrollar y documentar las actividades para recibir información, detectar o determinar una violación interna a la seguridad de la información (ver 8.1.24, lineamientos para la protección de la propiedad intelectual y de retención de registros).

Se debe desarrollar en articulación con los procesos de Gestión TIC, Investigación y Judicialización y Control Disciplinario, para el cumplimiento conjunto del presente lineamiento y del No. 8.3.4.

8.6.15. Desarrollar coordinadamente con los procesos del SGI, las actividades necesarias para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información y seguridad digital, y el establecimiento del SGSISD en la entidad, como son:

- Planificación y preparación de respuesta a incidentes.
- Seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad de la información.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 66 de 111

- Recolección y manejo de EMP⁷¹ de incidente de seguridad de la información.
- Valoración y toma de decisiones sobre eventos de seguridad de la información y valoración de debilidades.
- Respuesta y recuperación controlada de incidentes.

Nota. El presente lineamiento se debe desarrollar en coordinación con el proceso de mejora continua, para apoyar a los procesos que requieran establecer actividades documentadas.

8.6.16. Desarrollar en conjunto los procesos Gestión TIC, Gestión Documental y los demás procesos del SGI las actividades documentadas para asegurar que se tiene un plan de continuidad de SI, que contenga:

- Los requisitos de SI y la continuidad de su gestión después de la materialización de un evento que la afecte como estados de crisis o desastres.
- Establecer e implementar las actividades para asegurar un nivel aprobado de seguridad de la información durante y después de una situación adversa, basado en los requisitos de continuidad de la gestión de la seguridad de la información.
- Evaluación de los controles de continuidad de seguridad de la información después de una situación adversa a intervalos regulares o después de presentarse cambios organizacionales (plan estratégico, organigrama, leyes, etc.), técnicos (implementación de nueva infraestructura tecnológica), procedimientos y procesos (cambio en los procesos o como se ejecutan), etc.


8.6.17. Velar y hacer seguimiento de que todos los sistemas de información de la entidad y la información de la entidad tengan su listado de requisitos de ley, reglamentarios y contractuales actualizado.

8.6.18. Apoyar a los procesos custodios técnicos en el desarrollo de la metodología para asegurar la protección de los registros emitiendo lineamientos de retención, almacenamiento, manejo y disposición.

8.6.19. Velar que se desarrollen e implementen las leyes y normas dictadas por el Gobierno Nacional, que sean de obligatorio cumplimiento para la FGN en cuanto a seguridad de la información y seguridad digital.

8.6.20. Proponer el desarrollo y la implementación de aquellas normas y leyes que no sean de obligatorio cumplimiento para la FGN, pero que se pueden adoptar como buenas prácticas de seguridad de la información y seguridad

⁷¹ EMP: Elemento Material Probatorio

 FISCALÍA <small>GENERAL DE LA NACIÓN</small>	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 67 de 111


digital, en colaboración y coordinación armónica con las demás entidades del sector, el estado y/o la región.

- 8.6.21. Desarrollar en conjunto con el proceso de Gestión TIC las actividades, políticas y documentos necesarios para implementar, en lo que compete a la entidad, el Modelo de Gobernanza de Seguridad Digital.
- 8.6.22. Desarrollar, implementar y hacer seguimiento y control en conjunto con el SGI, a todas las actividades necesarias para el desarrollo, continuidad y apropiación del SGSISD de la FGN.


8.7. SEGURIDAD DE LA INFORMACIÓN EN LAS CONTRATACIONES Y LAS RELACIONES CON LOS PORVEEDORES

El modelo de seguridad y privacidad de la información adoptado por la entidad, basado en el MSPI del MinTIC y en la familia de las normas ISO/IEC 27000, requiere se implementen controles con especial enfoque en las relaciones contractuales y con proveedores, que aseguren la confidencialidad e integridad de la información de la entidad a la cual se les autorizará el acceso, por lo cual el proceso de Gestión Contractual deberá incluir dentro de su proceso:

- 8.7.1. Dentro de las obligaciones contractuales de los proveedores, se deberá incluir el cumplimiento de las políticas, directrices y lineamientos de seguridad de la información de la entidad.
- 8.7.2. Los proveedores y contratistas a los que se les otorgue acceso a información crítica o confidencial deben firmar un acuerdo de confidencialidad y no divulgación, y se debe proteger el acceso a información con datos personales o sensibles.
- 8.7.3. Los acuerdos de confidencialidad y no divulgación, se deben revisar periódicamente y cada vez que haya cambios legales o normativos internos o externos que afecten el modelo de seguridad de la información adoptado por la entidad.
- 8.7.4. Los deberes de protección de la seguridad de la información deben aplicar para las fases precontractuales, contractuales y poscontractuales (antes, durante y después de firmado el contrato) y no pueden ser opcionales.
- 8.7.5. Los requisitos de seguridad de la información que se va a compartir (entregar o recibir) por parte de la entidad o del proveedor, se pueden acordar antes de la firma y perfeccionamiento del contrato, pero ningún acuerdo puede presentar excepciones a alguna de las políticas o directrices de seguridad de la información adoptadas por la entidad.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 68 de 111


- 8.7.6. Los requisitos de seguridad exigibles para los oferentes y proveedores deben ir plasmados en los estudios previos elaborados por el área técnica.
- 8.7.7. Se deben hacer cumplir las responsabilidades para resguardar la seguridad de la información aun después de terminado el acuerdo contractual, para lo cual, se deben identificar y definir las responsabilidades y en tiempo por el cual se deben cumplir. En la identificación de la responsabilidad de SI debiera estar presente el área técnica, ya que no toda la información a la que se le brinde acceso a un proveedor o contratista tiene la misma clasificación de criticidad o sensibilidad.
- 8.7.8. El área técnica dentro de los estudios previos debe establecer los acuerdos de seguridad de la información con el proveedor, el tipo de información a la que tendrá acceso, el tiempo de acceso permitido, las restricciones y responsabilidades, si se va a extraer, manipular, procesar o almacenar información el método permitido para hacerlo, entre otros necesarios para el control de riesgos de pérdida de confidencialidad o integridad de la información.
- 8.7.9. Para los proveedores de suministros de TI se deben establecer los criterios del numeral anterior, además de los propios según el tipo de servicio o recurso contratado, teniendo en cuenta la valoración de los riesgos para la infraestructura crítica y la información confidencial o sensible a la que tendrán acceso.
- 8.7.10. Dentro de la actividad de supervisión del contrato, se debe hacer seguimiento al cumplimiento de los acuerdos, requisitos y deberes acordados con el proveedor o contratista acerca de seguridad de la información; informar cualquier violación o incidente de seguridad de la información y aplicar los procedimientos establecidos para la recuperación de incidentes y respuesta a incidentes de seguridad de la información.
- 8.7.11. Cualquier cambio contractual que afecte o ponga en riesgo la seguridad de la información, se debe hacer de forma legal según la forma que determine el proceso de Gestión Contractual.
- 8.7.12. Verificar que los contratos o convenios, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 69 de 111

8.8. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS BIENES Y EQUIPOS

La seguridad de la información no es exclusiva de los elementos informáticos, por el contrario, como lo establecen las normas ISO/IEC 27000 se deben asegurar todos los activos físicos o informáticos que se usen para procesamiento o almacenamiento de información, en ese sentido, hablamos no solo de computadores o equipos electrónicos, sino de estructuras físicas, equipos de respaldo y suministro de servicios, elementos de trabajo y de oficina, entre otros. Teniendo lo anterior, se establecen lineamientos específicos dentro del SGSISD para ser adaptados a las actividades del proceso de Gestión de Bienes, los cuales se detallan a continuación.

- 8.8.1. Los derechos de acceso a las instalaciones o depende la entidad, se deben otorgar a los servidores nuevos o a los que se les de autorización de acceso, por según sea asignado por Gestión de Talento Humano o por el proceso al que pertenece.
- 8.8.2. Los derechos de acceso a instalaciones o dependencias de la Entidad deben ser revocados en el momento de la desvinculación del servidor, en la terminación del contrato o ser modificadas por reasignación de funciones, traslados, encargo, remplazo, etc.
- 8.8.3. En el proceso de identificación y valoración de los riesgos se deben tener en cuenta todos los espacios, circunstancia y equipos en los que pueda ser posible una vulneración a la seguridad de la información, por lo que se deben controlar las áreas de despacho, carga y descarga de insumos y proveedores (ver control A.11.1.6).
- 8.8.4. Se deben asegurar las áreas de procesamiento de información contra intrusión o acceso no autorizado, por lo que se deben identificar con su ubicación y dependiendo del nivel de criticidad, sensibilidad o confidencialidad que el proceso propietario dio a la información que allí se maneja, implementar controles para asegurar su confidencialidad, privacidad e integridad.
- 8.8.5. Se deben asegurar las áreas en donde se encuentra los equipos de suministros y los servicios de suministros como agua, electricidad, telecomunicaciones, alcantarillado, ventilación, aire acondicionado, etc., los cuales soportan la disponibilidad de la información; hacer identificación y valoración de riesgos físicos como acceso no autorizado, intrusión, terrorismo, desastres naturales, fallas por mantenimiento o manipulación indebida, etc., implementar los controles necesarios y diseñar un plan de continuidad y recuperación en caso de su materialización.


	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 70 de 111

- 8.8.6. El proceso en conjunto con Gestión TIC, asegurará el cableado de telecomunicaciones y el eléctrico que soporta servicios de comunicación; éste se debe controlar y proteger contra interceptación, daño e interferencia (ver *guía de implementación* del numeral 11.2.3. “Seguridad del cableado” de la ISO/IEC 27002:2015).
- 8.8.7. Se deberán documentar actividades y emitir lineamientos para el control del retiro de activos y de información, los equipos que contienen, almacenada o procesan información o soportan el suministro de servicios a procesos de comunicación e información, no se podrán retirar del área asignada y menos de las instalaciones de la Entidad, en este sentido, solo el personal autorizado podrá hacerlo (personal interno, externo o proveedores).
- 8.8.8. Dentro del plan de continuidad de seguridad de la información, se deben proyectar la necesidad de crecimiento de las instalaciones de almacenamiento y procesamiento de información; además de los equipos de servicio de suministros que soportar las comunicaciones y redes eléctricas, y gestionar las necesidades para cubrir la demanda futura.
- 8.8.9. Verificar y controlar el cumplimiento de los acuerdos de seguridad de la información con los proveedores de equipos de servicios de suministros y los demás a los que aplique, para mayor claridad se recomienda consultar la guía de implementación del numeral 15.1.3 “cadena de suministros de tecnologías de la información y comunicación de la norma ISO/IEC 27002:2015 y alinearlos con los numerales 8.7 (relación con proveedores) y 8.3 (seguridad de la información para la gestión de tecnología de la información y las comunicaciones), en lo que aplique a cada uno

8.9. SEGURIDAD DE LA INFORMACIÓN EN LOS PROCESOS MISIONALES

Los procesos misionales son propietarios de la información misional de la entidad, o como dice la norma ISO/IEC 27001:2013 “la información de negocio”, esta información es la base del ser misional de la entidad, sin ella no tendría un propósito la FGN, por tal motivo es la que requiere más protección y controles ya que no solo está protegida por la ley si no que su divulgación, manipulación o acceso no autorizados, conllevaría riesgos catastróficos a nivel nacional, judicial, social y en los peores casos pondría en riesgo la vida de los intervinientes.

Los procesos misionales están conformados por cuatro procesos y dos subprocesos, el primero, Gestión de Denuncias y Análisis de la Información quien es propietaria de la información de entrada de la entidad, controla aplicaciones y sistemas de información, información física y documentada, de igual manera maneja

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 71 de 111

y ejerce custodia de la información de los casos penales mientras están bajo el control de intervención temprana.

El segundo, el proceso de Investigación y Judicialización, el cual procesa la información de los procesos penales de la entidad basados en las leyes 906 y 600, ejerce el rol de propietario de dicha información para lo cual cuenta con bases de datos, aplicaciones, sistemas informáticos, archivos, documentos e información almacenada en medios físicos y digitales. También, ejerce el rol y la responsabilidad como propietario y custodio técnico y funcional de la información almacenada en las *bodegas de evidencia*, para las cuales los controles de seguridad de la información, por la naturaleza de ésta, deben ser estrictos en la implementación y la aplicación.

El tercero es el Subproceso de Criminalística, el cual pertenece según el mapa de proceso de la entidad al proceso de Investigación y Judicialización, es el encargado de producir información crítica y sensible para el proceso penal, basa su gestión en la producción y procesamiento de la información necesaria resolutoria y argumentativa de casos penales.


El cuarto es el Subproceso de Protección y Asistencia, pertenece al proceso de Investigación y Judicialización y ejerce el rol de propietario de la información del programa de protección y asistencia y de los vinculados a éste; dicha información, se debe considerar como crítica, sensible y confidencial, teniendo en cuenta las características de los vinculados al programa, personas en riesgo o que su vida corre peligro por estar vinculadas a un proceso penal.

El quinto es el proceso de Justicia Transicional, propietario o responsable de la información de los procesos y las personas vinculadas a las investigaciones en contra de los miembros de las GAOML⁷² que se hayan desmovilizado o y aquellos postulados en el marco de los procesos de paz.


El sexto y último proceso, es el de Extinción del Derecho de Dominio, desarrolla el rol de propietario y custodio funcional de la información resultante de la acción de extinción de derecho de dominio dentro del proceso penal.

Los procesos misionales son propietario y custodios funcionales de la información crítica y sensible de la entidad, en consecuencia, deben implementar, apropiar y hacer seguimiento sin excepción, a los lineamientos de cumplimiento descritos en el numeral 8.1 de este manual, además deben identificar e implementar, aquellos controles propios después de la valoración de los riesgos de seguridad de la información, para lo cual tendrán en cuenta:

⁷² GAOML: Grupos Armados Organizados al Margen de la Ley

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 72 de 111


- 8.9.1. Conformar grupos encargados de la gestión, implementación y apropiación del SGSISD en su proceso.
- 8.9.2. Los grupos encargados de la gestión de seguridad de la información en los procesos misionales, se mantendrán actualizados acerca de las mejores prácticas en SI a través de grupos de interés especial que también, permita la comprensión del entorno actual de seguridad de la información.
- 8.9.3. La información almacenada en las bodegas de evidencias y las actividades de recolección y procesamiento de información, en alineación con el esquema de clasificación desarrollado por Gestión Documental y en cumplimiento al manual de cadena de custodia, implementarán procedimientos para el manejo de los medios removibles, por lo que debe tener en cuenta, según sea aplicable:
- Llevar registro del retiro de medios de su lugar de almacenamiento.
 - Almacenar los medios de manera segura según las especificaciones del fabricante.
 - Uso de técnicas criptográficas para la protección de los datos importantes con el fin de proteger la confidencialidad y la integridad de la información de las bodegas de evidencia.
 - Mitigar el riesgo de ilegibilidad de los datos por degradación de los medios, por lo que se desarrollaran actividades de control y transferencia.
 - Evaluar la posibilidad de implementar en ciertas actividades de recolección, procesamiento o custodia de información, la producción de más de una copia de los datos valiosos en medios separados, para reducir el riesgo de daño o pérdida.
 - Desarrollar un modelo de registro y control de medios para prevenir la pérdida de datos o el uso no autorizado.
 - Identificar en que actividades es válido o necesario el uso de medios removibles y autorizar su uso. Negar el uso de medios y controlarlo, en las actividades no autorizadas.
 - Hacer seguimiento de la transferencia de información entre medios removibles, concientizar acerca del uso permitido y de los riesgos asociados por pérdida o divulgación no autorizada.
 - Establecer actividades documentadas para la disposición segura de los medios con el fin de minimizar la fuga de información a personas no autorizadas y asegurar que la información no sea recuperable. Se pueden contemplar técnicas de borrado de datos, sin embargo, para la información crítica o confidencial, se deben evaluar técnicas de destrucción del medio como, por ejemplo, incineración.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 73 de 111

- Identificar los medios que requerirán una disposición segura y mantener registro.
- Los dispositivos dañados con información confidencias, critica o sensible, deberán ser evaluados para determinar su disposición final y asegurar que la información allí almacenada no podrá ser extraída por diferentes técnicas.
- Los métodos de disposición segura por destrucción o borrado y recolección, deberán estar alineadas con el Sistema de Gestión de Seguridad Ambiental de la Entidad.
- Asegurar que los medios de transporte o mensajería por la que se envían o reciben medio removibles, es segura y confiable.
- Asegurar que el embalaje del medio lo protegerá contra daño físico durante el transporte.
- Estructurar la información de las bodegas de evidencia para que pueda ser integrar dentro del lago de datos de la FGN.


8.9.4. Proteger las áreas de procesamiento o almacenamiento de información confidencial, critica o sensible, contra posibles daños y acceso no autorizado, tener en cuenta una vez identificadas:

- Fortalecer la seguridad física estableciendo los perímetros de seguridad de las instalaciones de recolección, procesamiento o almacenamiento de información; la seguridad implementada, estará basada en el resultado de la valoración de los riesgos y la criticidad y confidencialidad de la información que se maneje en cada área y según su ubicación.
- Los perímetros de una edificación en la que se encuentre un área de recolección, procesamiento o almacenamiento de información, deberán ser físicamente seguros, teniendo en cuenta techos, paredes, pisos, puertas seguras contra acceso no autorizado, ventanas, etc., no deberían tener brechas de seguridad que faciliten una intrusión.
- Restringir el acceso a estas áreas al personal autorizado y mantener vigilancia y control sobre los ingresos.
- Prevenir la contaminación ambiental de estas áreas y de ser necesario, construir barreras físicas que impidan el acceso físico no autorizado.
- Asegurarse o de lo contrario gestionar, que las áreas de recolección, procesamiento o almacenamiento de información cuentan con sistemas de control de incendios y actividades para reaccionar ante estos eventos.
- Si se cuentan con áreas de recolección, almacenamiento o procesamiento de información gestionadas por terceras partes, éstas deberán estar

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 74 de 111

separadas de las propias y se deberá exigir el cumplimiento y aplicación de los controles de SI a los terceros.


- Las áreas de procesamiento información crítica o confidencial deberían estar aseguradas para que las actividades y la información no sean visibles o audibles desde el exterior.
- 8.9.5. El Departamento de Seguridad deberá asegurar que se tienen identificados e implementados los controles de acceso físico a todas las instalaciones de la entidad, en cumplimiento de los objetivos del SGSISD.
- 8.9.6. El Departamento de Seguridad desarrollará directrices para mantener la seguridad física en oficinas, áreas e instalaciones de la entidad, para lo cual tendrá en cuenta:
- Identificar las áreas claves que requieran más seguridad por la criticidad y confidencialidad de la información que se maneje allí, éstas deberán estar ubicadas de manera que se restrinja y controle el acceso al público.
 - Mantener, en la medida de lo posible, confidencialidad y no señalización de la ubicación de las áreas críticas de procesamiento de información.
- 8.9.7. Con base en los resultados de la valoración de riesgos a instalaciones físicas, se deberá proponer la adecuada protección física contra desastres naturales en las áreas de procesamiento o almacenamiento de información.
- 8.9.8. Diseñar procedimientos que garanticen el trabajo en áreas seguras, aplicable a aquellas de manejo, procesamiento o almacenamiento de información, según la criticidad, confidencialidad de ésta.
- 8.9.9. Los equipos que manejan o contienen información se deberán ubicar de forma segura, de tal manera que las personas no autorizadas no puedan ver la información durante su uso.
- 8.9.10. Se deben adoptar directrices para proteger los equipos contra amenazas físicas, ambientales o descuidos de los custodios.
- 8.9.11. Se deben controlar los cambios en los procesos, actividades, servicios o en la infraestructura para evitar la afectación a la seguridad de la información. Si ocurren cambios significativos se deben identificar y registrar, los cambios deberían ser planificados y puestos a prueba, valorando los impactos en la seguridad de la información; de ser necesario se deberán reevaluar los riesgos y los controles.
- 8.9.12. El evaluar las necesidades de la Entidad y planificar la seguridad de la información que se requerirá con base en su crecimiento, asegura la capacidad de respuesta futura, por lo que los requerimientos para asegurar la continuidad y el crecimiento de la seguridad de la información se deberían incluir en los proyectos de inversión.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 75 de 111

- 8.9.13. Se deben identificar las áreas, servicio o actividades en las que se puede ver comprometida la confidencialidad o la integridad de la información por parte de servidores o terceros, diseñar y revisar de acuerdo con el área, servicio o actividad, acuerdos de confidencialidad y no divulgación en los que se especifiquen los deberes, las responsabilidades, los permisos y privilegios otorgados y las consecuencias por el mal uso de éstos (ver *guía de implementación* del numeral 13.2.4, ISO/IEC 27002:2015).
- 8.9.14. Apoyar en el desarrollar de los procedimientos de respuesta a incidentes de seguridad de la información, en especial en lo que compete a la revisión y recolección de evidencia forense, identificación de comisión de delitos e inicio de procesos penales.
- 8.9.15. Implementar las metodologías y herramientas necesarias para que la información de las bodegas de evidencia pueda ser integrada al lago de datos de la FGN, conforme a las políticas y lineamiento de gobierno de datos establecidas por la Dirección de Políticas y Estrategia.

8.10. GESTIÓN JURÍDICA Y COMUNICACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- 8.10.1. Gestión Jurídica como proceso de apoyo, contribuye en el desarrollo de la documentación de SGSISD que requiere soporte legal, en este sentido hará parte del equipo de trabajo para:
- 8.10.1.1. Diseño y desarrollo de los acuerdos de confidencialidad o de no divulgación que se implementen para usuarios internos y externos con acceso autorizado a la información de la entidad, proveedores, personal desvinculado pero que debe mantener reserva sobre la información, entre otros que se aprueben durante el proceso de desarrollo e implementación del sistema o sus revisiones.
- 8.10.1.2. El diseño y desarrollo de las Directrices para la protección de la propiedad intelectual (consultar como referencia anexo 1.2), documentación y lineamientos asociados basados en la *guía de implementación* del numeral 18.1.2 de la ISO/IEC 27002:2015.
- 8.10.1.3. Apoyar a la MTOGD, al Oficial de Seguridad y al responsable de la Estrategia de Seguridad de la Información en:
- a) Asesorar a los procesos de la Entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionadas con SI.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 76 de 111

- b) Asesorar a la MTOGD en temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionadas con SI.

8.10.2. Comunicación y Relacionamiento Institucional

La comunicación de la seguridad de la información es un requisito y parte de la estrategia de apropiación del sistema, por lo que el proceso de Comunicación y Relacionamiento Institucional en conjunto con el de Planeación Estratégica, desarrollará e implementará la estrategia de comunicación de las políticas, directrices y campañas de divulgación del SGSISD.

8.11. AUDITORÍA Y CONTROL DISCIPLINARIO

Los procesos de Auditoría y Control Disciplinario como parte del SGSISD deben apropiar los lineamientos de cumplimiento del numeral 8.1; además de desarrollar e implementar los de su competencia, como son:

8.11.1. Control Disciplinario

- Se implementarán actividades documentadas que permitan emprender acciones contra los servidores públicos que hayan cometido una violación contra la seguridad de la información, control A.7.2.3 “Proceso Disciplinario”.


8.11.2. Auditoría

- Una vez terminado el ciclo de operación del modelo y pasada la etapa de operatividad (numeral 6.1), realizará la revisión del SGSISD basado en el modelo de seguridad de la información adoptado por la entidad

9. COMPROMISOS DE LA ALTA DIRECCIÓN

Se entiende como compromiso de la Alta Dirección (inglés: Management commitment), el alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora del SGSISD. La versión de 2013 de ISO/IEC 27001 lo engloba bajo la cláusula de Liderazgo⁷³.

⁷³ <https://www.iso27000.es/glosario.html>

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 77 de 111


Por lo anterior, la Alta Dirección, en cabeza de señor Fiscal General de la Nación o su representante, realizará el seguimiento al Sistema de Gestión de Seguridad de la Información conforme a los requisitos de la norma ISO/IEC 27001:2013 y al Anexo 1 de MSPI del MinTIC.

9.1. COMPROMISOS Y LIDERAZGO DE LA ALTA DIRECCIÓN

9.1.1 Deberá revisar y aprobar la Política General de SI, así como las políticas, lineamiento, directrices y documentación seguridad de la información y seguridad digital que se desarrollen e implementen en cumplimiento de los requisitos de los estándares adoptados por la Entidad para el SGSISD. Las políticas y directrices de seguridad de la información deberán ser desarrolladas, implementadas y revisadas por los procesos propietarios de las mismas, las cuales son (ver anexo 2):

- A. Política General de Seguridad de la Información
- B. Política de control de acceso, uso de redes y servicios de red
- C. Directrices de clasificación de la información
- D. Directrices de seguridad física y de entorno
- E. Directrices de uso aceptable de activos
- F. Política de escritorio y pantalla limpios
- G. Política de transferencia de información y seguridad de las comunicaciones
- H. Política de dispositivos móviles y teletrabajo
- I. Política de prohibición de uso e instalación de software no autorizado
- J. Política de copias de respaldo
- K. Política de controles criptográficos, uso, protección y tiempo de vida de las llaves criptográficas
- L. Directrices de privacidad y protección de la información de datos personales
- M. Política de seguridad de la información en la relación con los proveedores
- N. Directrices de retención de registros
- O. Política de desarrollo seguro.
- P. Directrices para la protección de la propiedad intelectual.
- Q. Política de integridad de la información

Nota. Las políticas y directrices de SI se desarrollan en uno o más documento independiente en los que pueden estar consolidadas algunas, deben ser adoptadas por toda la entidad y hacen parte del plan de concientización, divulgación y capacitación del SGSISD. En el anexo

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 78 de 111

2, se encuentra la descripción de cada una, la relación con otros controles, los requisitos que deben cumplir (guía de implementación ISO/IEC 27002:2015), y el o los procesos propietarios.

- 9.1.2. Exigir a través de la Política General de SI, la adopción y cumplimiento de los lineamientos, directrices y políticas del SGSISD, en todos los procesos, áreas y niveles de la entidad, en servidores públicos interno o externos, contratistas, etc. Además de apoyar y promover su difusión y cumplimiento.
- 9.1.3. Reglamentar el Sistema de Seguridad de la Información de la FGN.
- 9.1.4. Reglamentar los roles y responsabilidades del SGSISD; definir sus funciones y asignarlas.
- 9.1.5. Planear y disponer de los recursos necesarios para la implementación y mantenimiento del SGSISD de la entidad, como son entre otros, presupuesto y personal.
- 9.1.6. Incluir dentro de los objetivos instituciones el desarrollo, implementación y mantenimiento del SGSISD.


10. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

La visión, la misión, la estrategia y los objetivos estratégicos de la entidad son el soporte de los principios de seguridad y privacidad de la información, por lo que se establece que:

- La información es los activos más importantes de la Fiscalía General de la Nación, por lo tanto, su utilización debe cumplir con la confidencialidad, integridad y disponibilidad acorde a las necesidades de la entidad.
- La confidencialidad de la información de la entidad y de terceras partes debe ser mantenida, independientemente del medio o formato donde se encuentre.
- La integridad de la información de la entidad debe ser preservada ya sea que esta se encuentre alojada de manera temporal o permanente, o del medio o mecanismo por el cual sea transmitida.
- La información de la entidad debe estar disponible cuando sea requerida.

11. ASPECTOS GENERALES

Para todos los efectos del presente manual y de todos los documentos, lineamientos, directrices y otros que se deriven del mismo, se entenderá que se basan, crean, desarrollan, implementan y adoptan con base en las versiones de las


	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 79 de 111

normas y estándares vigentes a la fecha de creación del presente manual, las cuales son:

1. ISO/IEC 27001:2013
2. ISO/IEC 27002:2015
3. ISO/IEC 27005:2020
4. Guía para la Administración de Riesgos y Diseño de Controles en Entidades Públicas, versión 5 de 2020, DAFP.
5. Modelo de Seguridad y Privacidad de la Información MPSI, versión 4 de 2021, MinTIC (corresponde al anexo 1 de la resolución 500 de 2021 del MinTIC).
6. Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD), 2018 MinTIC.

De ser requerido para actualización y mejora del SGSISD, de actualizará este manual a medida que cambien las versiones de las normas y estándares mencionados, conforme a las necesidades y posibilidades de la entidad.

Nota 1. Se excluye la Política General de Seguridad de la Información y su alcance que se adoptan mediante resolución del Fiscal General de la Nación

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 80 de 111


12. REVISIÓN Y APROBACIÓN

Adoptado mediante Resolución No. 008 del 28 de octubre de 2022.

	NOMBRE
Proyectó	Andrea González Ortega – Profesional DPD
Revisó	Adolfo Alexander Reyes – Profesional DPD Germán Bernal Valbuena - Profesional DPD Doris Maritza Chaparro Durán - Procesional DPD Eliana González Castillo – Profesional DPD
Aprobó	Gladys Eugenia Zambrano Arciniegas - Directora de Planeación y Desarrollo

Nota. Creación y revisión del documento

	Nombre	Cargo
Desarrollo	Andrea González Ortega	Profesional DPD
Revisión	Carolina Salgado Lozano	Director de Políticas y Estrategia
	Gladys Eugenia Zambrano Arciniegas	Directora de Planeación y Desarrollo
	Luis Fernando Lozano Mier	Subdirector de Tecnología de la Información y las Comunicaciones
	Germán Bernal Valbuena	Oficial de Seguridad - DPD
	Doris Maritza Chaparro Duran	Procesional DPD
	Samuel Paez Pisco	Profesional SI - SubTIC
	Equipo de trabajo Dirección de Políticas y Estrategia	Profesionales DPE

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 81 de 111

Anexo 1. Relación de cumplimiento ISO/IEC 27001:2013 - FGN

Anexo 1.1. Relación de cumplimiento ISO/IEC 27001:2013 – Procesos del Sistema

Requisito NTC: ISO/IEC 27001	Procesos estratégicos		Procesos y subprocesos misionales						Procesos de apoyo							Proceso de seguimiento, control y mejora			
	Número y descripción	PE	CRI	GDAI	IV	CR	PA	JT	ED	GC	GB	GTH	GD	GF	GJ	GTIC	MC	AU	CD
4. Contexto de la organización																			
4.1. Conocimiento de la organización y su contexto	4.1																		
4.2. Comprensión de las necesidades y expectativas de las partes interesadas	4.2																		
4.3. Determinación del alcance del SGSI	4.3																		
4.4. Sistema de Gestión de Seguridad de la Información	4.4														4.4				
5. Liderazgo																			
5.1. Liderazgo y compromiso	5.1															5.1			
5.2. Política	5.2														5.2				
5.3. Roles, responsabilidades y autoridades de la entidad	5.3														5.3				
6. Planificación																			
6.1. Acciones para tratar riesgos y oportunidades	6.1																		
6.1.1. Generalidades	6.1.1																		
6.1.2. Valoración de riesgos de la seguridad de la información	6.1.2	6.1.2	6.1.2	6.1.2	6.1.2	6.1.2	6.1.2	6.1.2	6.1.2	6.1.2	6.1.2	6.1.2	6.1.2	6.1.2	6.1.2	6.1.2	6.1.2	6.1.2	6.1.2
6.1.3. Tratamiento de riesgos de seguridad de la información	6.1.3	6.1.3	6.1.3	6.1.3	6.1.3	6.1.3	6.1.3	6.1.3	6.1.3	6.1.3	6.1.3	6.1.3	6.1.3	6.1.3	6.1.3	6.1.3	6.1.3	6.1.3	6.1.3
6.2. Objetivos de seguridad de la información y planes para lograrlos	6.2	6.2	6.2	6.2	6.2	6.2	6.2	6.2	6.2	6.2	6.2	6.2	6.2	6.2	6.2	6.2	6.2	6.2	6.2
7. Soporte																			
7.1. Recursos	7.1														7.1				



PROCESO PLANEACIÓN ESTRATÉGICA

MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD

Código: FGN-EP01-M-02

Versión: 01

Página: 82 de 111

7.2. Competencia	7.2										7.2								
7.3. Toma de conciencia	7.3	7.3													7.3				
7.4. Comunicación	7.4	7.4													7.4				
7.5. Información documentada																			
7.5.1 Generalidades	7.5.1	7.5.1	7.5.1	7.5.1	7.5.1	7.5.1	7.5.1	7.5.1	7.5.1	7.5.1	7.5.1	7.5.1	7.5.1	7.5.1	7.5.1	7.5.1	7.5.1	7.5.1	7.5.1
7.5.2. Creación y actualización	7.5.2	7.5.2	7.5.2	7.5.2	7.5.2	7.5.2	7.5.2	7.5.2	7.5.2	7.5.2	7.5.2	7.5.2	7.5.2	7.5.2	7.5.2	7.5.2	7.5.2	7.5.2	7.5.2
7.5.3. Control de la información documentada	7.5.3	7.5.3	7.5.3	7.5.3	7.5.3	7.5.3	7.5.3	7.5.3	7.5.3	7.5.3	7.5.3	7.5.3	7.5.3	7.5.3	7.5.3	7.5.3	7.5.3	7.5.3	7.5.3
8. Operación																			
8.1. Planificación y control operacional	8.1	8.1	8.1	8.1	8.1	8.1	8.1	8.1	8.1	8.1	8.1	8.1	8.1	8.1	8.1	8.1	8.1	8.1	8.1
8.2. Valoración de riesgos de seguridad de la información	8.2	8.2	8.2	8.2	8.2	8.2	8.2	8.2	8.2	8.2	8.2	8.2	8.2	8.2	8.2	8.2	8.2	8.2	8.2
8.3. Tratamiento de riesgo de seguridad de la información	8.3	8.3	8.3	8.3	8.3	8.3	8.3	8.3	8.3	8.3	8.3	8.3	8.3	8.3	8.3	8.3	8.3	8.3	8.3
9. Evaluación de desempeño																			
9.1. Seguimiento, medición, análisis y evaluación	9.1	9.1	9.1	9.1	9.1	9.1	9.1	9.1	9.1	9.1	9.1	9.1	9.1	9.1	9.1	9.1	9.1	9.1	9.1
9.2. Auditoría interna																			9.2
9.3. Revisión por la dirección	9.3														9.3				
10. Mejora																			
10.1. No conformidades y acciones correctivas	10.1	10.1	10.1	10.1	10.1	10.1	10.1	10.1	10.1	10.1	10.1	10.1	10.1	10.1	10.1	10.1	10.1	10.1	10.1
10.2. Mejora continua	10.2															10.2	10.2		

Anexo 1.2. Relación de cumplimiento de los controles del anexo A de la ISO/IEC 27001:2013

Para entender la tabla de relación entre los controles del anexo A de la ISO/IEC 27001:2013 y el sistema de gestión por procesos de la entidad, se ha creado la siguiente tabla y las convenciones de apropiación, implementación o desarrollo del control dentro del sistema.

Apropia (AP): Proceso encargado de aplicar el control bajo los lineamientos de desarrollo e implementación.

Implementa (IM): Proceso encargado implementar el control a través de políticas, lineamientos, procedimientos y formatos documentados, proyectos, programas, etc.

Desarrolla (DE): Proceso que DE solo o en conjunto la estrategia para la implementación del control y dicta los lineamientos para su adecuada implementación y apropiación.



PROCESO PLANEACIÓN ESTRATÉGICA

MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD

Código: FGN-EP01-M-02

Versión: 01

Página: 83 de 111

Descripción	Procesos estratégicos		Procesos y subprocesos misionales						Procesos de apoyo						Proceso de seguimiento, control y mejora			
	PE	CRI	GDAI	IV	CR	PA	JT	ED	GC	GB	GTH	GD	GF	GJ	GTIC	MC	AU	CD
Requisito NTC: ISO/IEC 27001																		
A.5.	Políticas de seguridad de la información																	
A.5.1.	Orientación de la dirección para la gestión de la seguridad de la información <i>Lineamiento: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.</i>																	
A.5.1.1.	DE/IM/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	AP	AP	AP
A.5.1.2.	DE/IM										DE/IM			DE/IM				
A.6.	Organización para la seguridad de la información																	
A.6.1.	Organización interna <i>Lineamiento: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.</i>																	
A.6.1.1.	DE/IM/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/AP	DE/AP	AP	AP
A.6.1.2.	DE/AP														DE/IM/AP			
A.6.1.3.	DE/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	AP	AP	AP
A.6.1.4.			IM/AP	IM/AP	IM/AP	IM/AP	IM/AP	IM/AP							DE/IM/AP			
A.6.1.5.	DE/IM/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
A.6.2.	Dispositivos móviles y teletrabajo <i>Lineamiento: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.</i>																	
A.6.2.1.	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	DE/IM/AP	AP	AP	AP	DE/IM/AP	AP	AP	AP
A.6.2.2.	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	DE/IM/AP	AP	AP	AP	DE/IM/AP	AP	AP	AP
A.7.	Seguridad de los recursos humanos																	
A.7.1.	Antes de asumir el empleo <i>Lineamiento: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.</i>																	
A.7.1.1.												DE/IM/AP						
A.7.1.2.									IM/AP		DE/IM/AP				DE			
A.7.2.	Durante la ejecución del empleo <i>Lineamiento: Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades y de seguridad de la información y las cumplan.</i>																	
A.7.2.1.	DE/IM/AP	AP	AP	AP	AP	AP	AP	AP	IM/AP	AP	IM/AP	AP	AP	AP	IM/AP	AP	AP	AP
A.7.2.2.	DE/IM	DE/IM									DE/IM				DE/IM			
A.7.2.3.	DE/IM/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/AP	AP	AP	AP	DE/AP	AP	AP	DE/IM/AP
A.7.3.	Terminación y cambio de empleo <i>Lineamiento: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.</i>																	
A.7.3.1.	DE/AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	AP	DE/IM/AP	AP	AP	AP	DE/AP	AP	AP	AP
A.8.	Gestión de activos																	
A.8.1.	Responsabilidad por los activos <i>Lineamiento: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.</i>																	
A.8.1.1.	DE/IM/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/AP	AP	AP	DE/IM/AP	AP	AP	AP



PROCESO PLANEACIÓN ESTRATÉGICA

MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD

Código: FGN-EP01-M-02

Versión: 01

Página: 84 de 111

A.8.1.2.	Propiedad de los activos	DE/IM/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/AP	AP	AP	DE/IM/AP	AP	AP	AP
A.8.1.3.	Uso aceptable de activos	DE/IM/AP	AP	AP	DE/AP	AP	AP	AP	AP	AP	AP	AP	DE/AP	AP	AP	DE/IM/AP	AP	AP	AP
A.8.1.4.	Devolución de activos	DE/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	AP	AP	AP	DE/IM/AP	AP	AP	AP
A.8.2.	Clasificación de la información	<i>Lineamiento: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.</i>																	
A.8.2.1.	Clasificación de la información	DE/IM/AP	IM/AP	IM/AP	IM/AP	IM/AP	IM/AP	IM/AP	IM/AP	IM/AP	IM/AP	IM/AP	IM/AP	IM/AP	IM/AP	IM/AP	IM/AP	IM/AP	IM/AP
A.8.2.2.	Etiquetado de la información	DE/IM/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/AP	AP	AP	DE/AP	AP	AP	AP
A.8.2.3.	Manejo de activos de información	DE/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	AP	AP	DE/IM/AP	AP	AP	AP
A.8.3.	Manejo de medios	<i>Lineamiento: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios</i>																	
A.8.3.1.	Gestión de medios removibles	AP	AP	AP	DE/IM/AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	AP	AP	DE/IM/AP	AP	AP	AP
A.8.3.2.	Disposición de los medios	AP	AP	AP	DE/IM/AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	AP	AP	DE/IM/AP	AP	AP	AP
A.8.3.3.	Transferencia de los medios físicos	AP	AP	AP	DE/IM/AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	AP	AP	DE/IM/AP	AP	AP	AP
A.9.	Control de acceso																		
A.9.1.	Requisitos de negocio para el control de accesos	<i>Lineamiento: Limitar el acceso a información y a instalaciones de procesamiento de información.</i>																	
A.9.1.1.	Política de control de acceso	DE/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	AP	AP	DE/IM/AP	AP	AP	AP
A.9.1.2.	Acceso a redes y a servicios de red	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	AP	AP	AP
A.9.2.	Gestión de acceso de usuarios	<i>Lineamiento: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.</i>																	
A.9.2.1.	Registro y cancelación del registro de usuario	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	AP	AP	AP
A.9.2.2.	Suministro de acceso a usuario	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	AP	AP	AP
A.9.2.3.	Gestión de derechos de acceso privilegiado	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	AP	AP	AP
A.9.2.4.	Gestión de autenticación secreta de usuario (Management of Secret Authentication Information of Users)	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	AP	AP	AP
A.9.2.5.	Revisión de los derechos de acceso a usuarios	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	AP	AP	DE/IM/AP	AP	AP	AP
A.9.2.6.	Retiro y ajuste de los derechos de acceso	AP	AP	AP	AP	AP	AP	AP	AP	AP	IM/AP	DE/IM/AP	AP	AP	AP	DE/IM/AP	AP	AP	AP
A.9.3.	Responsabilidades de los usuarios	<i>Lineamiento: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.</i>																	
A.9.3.1.	Uso de información de autenticación secreta	DE/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	AP	AP	AP
A.9.4.	Control de acceso a sistemas y aplicaciones	<i>Lineamiento: Evitar el acceso no autorizado a sistemas y aplicaciones.</i>																	
A.9.4.1.	Restricción de acceso a la información															DE/IM/AP			
A.9.4.2.	Procedimiento de ingreso seguro															DE/IM/AP			
A.9.4.3.	Sistema de gestión de contraseñas															DE/IM/AP			
A.9.4.4.	Uso de programas utilitarios privilegiados	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/AP	AP	AP	AP

A.9.4.5.	Control de acceso a códigos fuente de programas																			DE/IM/ AP
A.10.	Criptografía																			
A.10.1.	Controles criptográficos	Lineamiento: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.																		
A.10.1.1.	Política sobre el uso de controles criptográficos	DE/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/ AP
A.10.1.2.	Gestión de llaves	DE/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/ AP
A.11.	Seguridad física y entorno																			
A.11.1.	Áreas seguras	Lineamiento: Prevenir el acceso físico no autorizado, el daño y la interferencia de la información y las instalaciones de procesamiento de información de la Entidad.																		
A.11.1.1.	Perímetro de seguridad física	DE/AP	DE/AP	DE/AP	DE/IM/ AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP
A.11.1.2.	Controles de acceso físico	DE/AP	DE/AP	DE/AP	DE/IM/ AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP
A.11.1.3.	Seguridad de oficinas, recintos e instalaciones	DE/AP	DE/AP	DE/AP	DE/IM/ AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP
A.11.1.4.	Protección contra amenazas externas y ambientales	DE/AP	DE/AP	DE/AP	DE/IM/ AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP
A.11.1.5.	Trabajo en áreas seguras	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP
A.11.1.6.	Áreas de despacho y carga																			DE/IM/ AP
A.11.2.	Equipos	Lineamiento: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la Entidad.																		
A.11.2.1.	Ubicación y protección de equipos				DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP			DE/IM/ AP							DE/IM/ AP
A.11.2.2.	Servicios de suministros												DE/IM/ AP							DE/IM/ AP
A.11.2.3.	Seguridad de cableado												DE/IM/ AP							DE/IM/ AP
A.11.2.4.	Mantenimiento de equipos												DE/IM/ AP							DE/IM/ AP
A.11.2.5.	Retiro de activos	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/ AP	AP	AP	AP	AP	AP	DE/IM/ AP	AP
A.11.2.6.	Seguridad de equipos y activos fuera de las instalaciones	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/ AP	AP	AP	AP	AP	DE/IM/ AP	AP
A.11.2.7.	Disposición segura o reutilización de equipos																			DE/IM/ AP
A.11.2.8.	Equipos de usuario desatendido	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/ AP	AP
A.11.2.9.	Política de escritorio limpio y pantalla limpia	DE/IM/ AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
A.12.	Seguridad de las operaciones																			
A.12.1.	Procedimiento operacionales y responsabilidades	Lineamiento: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.																		
A.12.1.1.	Procedimientos operacionales y responsabilidades	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/ AP	AP
A.12.1.2.	Gestión de cambios	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP	DE/IM/ AP
A.12.1.3.	Gestión de capacidad			DE/AP	DE/AP	DE/AP	DE/AP	DE/AP	DE/AP											DE/IM/ AP
A.12.1.4.	Separación de ambientes de desarrollo, pruebas y operación			AP	AP	AP	AP	AP	AP											DE/IM/ AP



PROCESO PLANEACIÓN ESTRATÉGICA

MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD

Código: FGN-EP01-M-02

Versión: 01

Página: 86 de 111

A.12.2.	Protección contra códigos maliciosos	<i>Lineamiento: Asegurar que de la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.</i>																			
A.12.2.1.	Controles contra códigos maliciosos	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/	AP	AP	AP
A.12.3.	Copias de respaldo	<i>Lineamiento: Proteger contra la pérdida de datos.</i>																			
A.12.3.1.	Respaldo de la información	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/	AP	AP	AP	DE/IM/	AP	AP	AP
A.12.4.	Registro y seguimiento	<i>Lineamiento: Registrar eventos y generar evidencias.</i>																			
A.12.4.1.	Registro de eventos																	DE/IM/			
A.12.4.2.	Protección de la información de registros																	DE/IM/			
A.12.4.3.	Registros del administrador y del operador																	DE/IM/			
A.12.4.4.	Sincronización de relojes.																	DE/IM/			
A.12.5.	Control de software operacional	<i>Lineamiento: Asegurarse de la integridad de los sistemas operacionales.</i>																			
A.12.5.1.	Instalación de software en sistemas operativos																	DE/IM/			
A.12.6.	Gestión de vulnerabilidad técnica	<i>Lineamiento: Prevenir el aprovechamiento de las vulnerabilidades técnicas.</i>																			
A.12.6.1.	Gestión de las vulnerabilidades técnicas																	DE/IM/			
A.12.6.2.	Restricción sobre la instalación de software	DE/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/	AP	AP	AP
A.12.7.	Consideraciones sobre auditorías de sistemas de información	<i>Lineamiento: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.</i>																			
A.12.7.1.	Controles de auditorías de sistemas de información																	DE/IM/			
A.13.	Seguridad de las comunicaciones																				
A.13.1.	Gestión de la seguridad de las redes	<i>Lineamiento: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.</i>																			
A.13.1.1.	Controles de redes																	DE/IM/			
A.13.1.2.	Seguridad de los servicios de red																	DE/IM/			
A.13.1.3.	Separación en las redes																	DE/IM/			
A.13.2.	Transferencia de información	<i>Lineamiento: Mantener la seguridad de la información transferida dentro de la Entidad y con cualquier entidad externa.</i>																			
A.13.2.1.	Políticas y procedimientos de transferencia de información	DE/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/	DE/AP	AP	AP
A.13.2.2.	Acuerdos sobre transferencia de información	DE/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/	AP	AP	AP
A.13.2.3.	Mensajería electrónica																	DE/IM/			
A.13.2.4.	Acuerdos de confidencialidad o de no divulgación	DE/AP	AP	AP	DE/IM/	AP	AP	AP	AP	DE/IM/	AP	DE/IM/	AP	AP	DE/AP			DE/IM/	AP	AP	AP
A.14.	Adquisición, desarrollo y mantenimiento de sistemas																				
A.14.1.	Requisitos de seguridad de los sistemas de información	<i>Lineamiento: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.</i>																			
A.14.1.1.	Análisis y especificación de requisitos de seguridad de la información																	DE/IM/			



PROCESO PLANEACIÓN ESTRATÉGICA


MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD

Código: FGN-EP01-M-02

Versión: 01


Página: 88 de 111

A.16.1.2.	Reporte de eventos de seguridad de la información	DE/IM/ AP	AP	AP	DE/IM/ AP	AP	AP	AP	AP	AP	AP	AP	DE/AP	AP	AP	DE/AP	AP	AP	AP	
A.16.1.3.	Reporte de debilidades de seguridad de la información	DE/IM/ AP	AP	AP	DE/IM/ AP	AP	AP	AP	AP	AP	AP	AP	DE/AP	AP	AP	DE/AP	AP	AP	AP	
A.16.1.4.	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	DE/IM/ AP	AP	AP	DE/IM/ AP	AP	AP	AP	AP	AP	AP	AP	DE/AP	AP	AP	DE/AP	AP	AP	AP	
A.16.1.5.	Respuesta a incidentes de seguridad de la información	DE/IM/ AP	AP	AP	DE/IM/ AP	AP	AP	AP	AP	AP	AP	AP	DE/AP	AP	AP	DE/AP	AP	AP	AP	
A.16.1.6.	Aprendizaje obtenido de los incidentes de seguridad de la información	DE/IM/ AP	AP	AP	DE/IM/ AP	AP	AP	AP	AP	AP	AP	AP	DE/AP	AP	AP	DE/AP	AP	AP	AP	
A.16.1.7.	Recolección de evidencia	DE/IM/ AP	AP	AP	DE/IM/ AP	AP	AP	AP	AP	AP	AP	AP	DE/AP	AP	AP	DE/AP	AP	AP	AP	
A.17.	Aspectos de seguridad de la información de la gestión de continuidad de negocio																			
A.17.1.	Continuidad de seguridad de la información	Lineamiento: La comunicación de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.																		
A.17.1.1.	Planificación de la continuidad de la seguridad de la información	DE/IM/ AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/ AP	AP	DE/IM/ AP	AP	AP	DE/IM/ AP	DE/IM/ AP	AP	AP
A.17.1.2.	Implementación de la continuidad de la seguridad de la información	DE/IM/ AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/ AP	AP	AP	DE/IM/ AP	AP	AP	AP	AP
A.17.1.3.	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	DE/IM/ AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/ AP	AP	AP	DE/IM/ AP	AP	AP	AP	AP
A.17.2.	Redundancias																			
A.17.2.1.	Disponibilidad de instalaciones de procesamiento de información.															DE/IM/ AP				
A.18.	Cumplimiento																			
A.18.1.	Cumplimiento de requisitos legales y contractuales	Lineamiento: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad.																		
A.18.1.1.	Identificación de la legislación aplicable y de los requisitos contractuales	DE/IM/ AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/ AP	AP	AP	IM/AP	AP	AP	AP	AP
A.18.1.2.	Derechos de propiedad intelectual	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/ AP	AP	DE/IM/ AP	DE/IM/ AP	AP	AP	AP	AP
A.18.1.3.	Protección de registros	DE/AP	AP	AP	DE/IM/ AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/ AP	AP	AP	DE/IM/ AP	AP	AP	AP	AP
A.18.1.4.	Privacidad y protección de datos personales	DE/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/ AP	AP	AP	DE/IM/ AP	DE/AP	AP	AP	AP
A.18.1.5.	Reglamentación de controles criptográficos	DE/AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	DE/IM/ AP	AP	AP	AP	AP
A.18.2.	Revisiones de seguridad de la información	Lineamiento: Asegurar que la seguridad de la información se IM y opera de acuerdo con las políticas y procedimientos organizacionales.																		
A.18.2.1.	Revisión independiente de la seguridad de la información	DE/IM/ AP																	DE/IM/ AP	
A.18.2.2.	Cumplimiento con las políticas y normas de seguridad	DE/IM/ AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
A.18.2.3.	Revisión del cumplimiento técnico															DE/IM/ AP				


	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 89 de 111

Anexo 1.3. Anexo A ISO/IEC 27001:2013


Anexo A - ISO/IEC 27001:2013		
Núm..	Control	Descripción
A.5.	Políticas de seguridad de la información	
A.5.1.	Orientación de la dirección para la gestión de la seguridad de la información	Lineamiento: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
<i>Objetivo: Brindar orientación y soporte, por parte de la dirección a la seguridad de la información</i>		
A.5.1.1.	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobadas por la dirección, publicada y comunicada a los empleados y partes externas pertinentes
A.5.1.2.	Revisión de las políticas para la seguridad de la información	Control: Las políticas para seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
A.6.	Organización para la seguridad de la información	
A.6.1.	Organización interna	Lineamiento: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
<i>Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información en la Entidad</i>		
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2.	Separación de deberes (segregación de funciones)	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3.	Contacto con las autoridades	Control: Se deben mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4.	Contacto con grupos de interés especial	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.1.5.	Seguridad de la información para la gestión de proyectos	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2.	Dispositivos móviles y teletrabajo	Lineamiento: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.
<i>Objetivo: Organizar la seguridad del teletrabajo y el uso de dispositivos móviles</i>		
A.6.2.1.	Política de dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2.	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 90 de 111


A.7.	Seguridad de los recursos humanos	
A.7.1.	Antes de asumir el empleo	Lineamiento: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
<i>Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.</i>		
A.7.1.1.	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.1.2.	Términos y condiciones de empleo	Control: Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2.	Durante la ejecución del empleo	Control: Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
<i>Objetivo: Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades y de seguridad de la información y las cumplan.</i>		
A.7.2.1.	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2.	Toma de conciencia, educación y formación en la seguridad de la información	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberán recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.7.2.3.	Proceso disciplinario	Control: Se debe contar con un proceso disciplinario formal el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3.	Terminación y cambio de empleo	Lineamiento: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.
<i>Objetivo: Proteger los intereses de la Entidad como parte del proceso de cambio o terminación del empleo</i>		
A.7.3.1.	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de contrato se deben definir, comunicar al empleado o contratista y se deberían hacer cumplir.
A.8.	Gestión de activos	
A.8.1.		Lineamiento: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
<i>Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas</i>		

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 91 de 111


A.8.1.1.	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
A.8.1.2.	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.
A.8.1.3.	Uso aceptable de activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4.	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2.	Clasificación de la información	Lineamiento: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.
<i>Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la Entidad.</i>		
A.8.2.1.	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2.	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.2.3.	Manejo de activos de información	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.3.	Manejo de medios	
<i>Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios</i>		
A.8.3.1.	Gestión de medios removibles	Control: Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2.	Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3.	Transferencia de los medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9.	Control de acceso	
A.9.1.	Requisitos de negocio para el control de accesos	Lineamiento: Limitar el acceso a información y a instalaciones de procesamiento de información.
<i>Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.</i>		
A.9.1.1.	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 92 de 111


A.9.1.2.	Acceso a redes y a servicios de red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2.	Gestión de acceso de usuarios	Lineamiento: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
<i>Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso a los usuarios no autorizados a sistemas y servicios.</i>		
A.9.2.1.	Registro y cancelación del registro de usuario	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2.	Suministro de acceso a usuario	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3.	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4.	Gestión de autenticación secreta de usuario (Management of Secret Authentication Information of Users)	Control: La asignación de la información secreta se debe controlar por medio de un proceso de gestión formal.
A.9.2.5.	Revisión de los derechos de acceso a usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6.	Retiro y ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.
A.9.3.	Responsabilidades de los usuarios	Lineamiento: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
<i>Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.</i>		
A.9.3.1.	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4.	Control de acceso a sistemas y aplicaciones	Lineamiento: Evitar el acceso no autorizado a sistemas y aplicaciones.
<i>Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.</i>		
A.9.4.1.	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
A.9.4.2.	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.
A.9.4.3.	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
A.9.4.4.	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 93 de 111


A.9.4.5.	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.
A.10.	Criptografía	
A.10.1.	Controles criptográficos	Lineamiento: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
<i>Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.</i>		
A.10.1.1.	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2.	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
A.11.	Seguridad física y entorno	
A.11.1.	Áreas seguras	Lineamiento: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización
<i>Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia de la información y las instalaciones de procesamiento de información de la Entidad.</i>		
A.11.1.1.	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.
A.11.1.2.	Controles de acceso físico	Control: Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
A.11.1.3.	Seguridad de oficinas, recintos e instalaciones	Control: Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4.	Protección contra amenazas externas y ambientales	Control: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5.	Trabajo en áreas seguras	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6.	Áreas de despacho y carga	Control: Se deben controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2.	Equipos	Lineamiento: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.
<i>Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la Entidad.</i>		
A.11.2.1.	Ubicación y protección de equipos	Control: Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 94 de 111


A.11.2.2.	Servicios de suministros	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.3.	Seguridad de cableado	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debe estar protegido contra interceptación, interferencia o daño.
A.11.2.4.	Mantenimiento de equipos	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.11.2.5.	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
A.11.2.6.	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7.	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
A.11.2.8.	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.
A.11.2.9.	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12.	Seguridad de las operaciones	
A.12.1.	Procedimiento operacionales y responsabilidades	Lineamiento: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
<i>Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.</i>		
A.12.1.1.	Procedimientos operacionales y responsabilidades	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.
A.12.1.2.	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.12.1.3.	Gestión de capacidad	Control: Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
A.12.1.4.	Separación de ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.12.2.	Protección contra códigos maliciosos	Lineamiento: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
<i>Objetivo: Asegurar que de la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.</i>		

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 95 de 111


A.12.2.1.	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.3.	Copias de respaldo	Lineamiento: Proteger contra la pérdida de datos.
<i>Objetivo: Proteger contra la pérdida de datos.</i>		
A.12.3.1.	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, del software de imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
A.12.4.	Registro y seguimiento	Lineamiento: Registrar eventos y generar evidencia.
<i>Objetivo: Registrar eventos y generar evidencias.</i>		
A.12.4.1.	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2.	Protección de la información de registros	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
A.12.4.3.	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deberían proteger y revisar con regularidad.
A.12.4.4.	Sincronización de relojes.	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
A.12.5.	Control de software operacional	Lineamiento: Asegurar la integridad de los sistemas operacionales
<i>Objetivo: Asegurarse de la integridad de los sistemas operacionales.</i>		
A.12.5.1.	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6.	Gestión de vulnerabilidad técnica	Lineamiento: Prevenir el aprovechamiento de las vulnerabilidades técnicas.
<i>Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.</i>		
A.12.6.1.	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2.	Restricción sobre la instalación de software	Control: Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.12.7.	Consideraciones sobre auditorías de sistemas de información	Lineamiento: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.
<i>Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.</i>		
A.12.7.1.	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13.	Seguridad de las comunicaciones	

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 96 de 111


A.13.1.	Gestión de la seguridad de las redes	Lineamiento: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
<i>Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.</i>		
A.13.1.1.	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.2.	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.1.3.	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
A.13.2.	Transferencia de información	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
<i>Objetivo: Mantener la seguridad de la información transferida dentro de la Entidad y con cualquier entidad externa.</i>		
A.13.2.1.	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
A.13.2.2.	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.3.	Mensajería electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4.	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14.	Adquisición, desarrollo y mantenimientos de sistemas	
A.14.1.	Requisitos de seguridad de los sistemas de información	Lineamiento: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.
<i>Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.</i>		
A.14.1.1.	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2.	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.

 FISCALÍA <small>GENERAL DE LA NACIÓN</small>	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 97 de 111


A.14.1.3.	Protección de transacciones de los servicios de las aplicaciones	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2.	Seguridad en los procesos de desarrollo y soporte	Lineamiento: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información
<i>Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.</i>		
A.14.2.1.	Política de desarrollo seguro	Control: Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
A.14.2.2.	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3.	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4.	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.
A.14.2.5.	Principios de construcción de sistemas seguros	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6.	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7.	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.14.2.8.	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9.	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A.14.3.	Datos de prueba	Lineamiento: Asegurar la protección de los datos usados para pruebas.
<i>Objetivo: Asegurar la protección de los datos usados para pruebas.</i>		
A.14.3.1.	Protección de datos de prueba	Control: Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 98 de 111


A.15.	Relación con los proveedores	
A.15.1.	Seguridad de la información en las relaciones con los proveedores	Lineamiento: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
<i>Objetivo: Asegurar la protección de los archivos de la organización que sean accesibles a los proveedores.</i>		
A.15.1.1.	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deberían documentar.
A.15.1.2.	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A.15.1.3.	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
A.15.2.	Gestión de la prestación de servicios con los proveedores	Lineamiento: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.
<i>Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación de servicio en línea con los acuerdos con los proveedores.</i>		
A.15.2.1.	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2.2.	Gestión de cambios en los servicios de proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos
A.16.	Gestión de incidentes de seguridad de la información	
A.16.1.	Gestión de incidentes y mejoras en la seguridad de la información	Lineamiento: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
<i>Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.</i>		
A.16.1.1.	Responsabilidad y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2.	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 99 de 111

A.16.1.3.	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A.16.1.4.	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5.	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6.	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.
A.16.1.7.	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17.	Aspectos de seguridad de la información de la gestión de continuidad de negocio	
A.17.1.	Continuidad de seguridad de la información	Lineamiento: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.
<i>Objetivo: La comunicación de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.</i>		
A.17.1.1.	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2.	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa
A.17.1.3.	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2.	Redundancias	Lineamiento: Asegurar la disponibilidad de instalaciones de procesamiento de información.
<i>Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.</i>		
A.17.2.1.	Disponibilidad de instalaciones de procesamiento de información.	Control: Las instalaciones de procesamiento de información se debe implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A.18.	Cumplimiento	


	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 100 de 111

A.18.1.	Cumplimiento de requisitos legales y contractuales	Lineamiento: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
<i>Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad.</i>		
A.18.1.1.	Identificación de la legislación aplicable y de los requisitos contractuales	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.1.2.	Derechos de propiedad intelectual	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1.3.	Protección de registros	Control: Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4.	Privacidad y protección de datos personales	Control: Cuando sea aplicable, se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
A.18.1.5.	Reglamentación de controles criptográficos	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinente.
A.18.2.	Revisiones de seguridad de la información	Lineamiento: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.
<i>Objetivo: Asegurar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos organizacionales.</i>		
A.18.2.1.	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2.	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2.3.	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.


 FISCALÍA <small>GENERAL DE LA NACIÓN</small>	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 101 de 111

Anexo 2. Políticas y directrices de seguridad de la información.


Políticas y Directrices de seguridad de la información		
A. Política General de Seguridad y Privacidad de la Información	Descripción	<p>La Política General de SI de la FGN, debe reflejar la intención es la alta dirección para implementarla y mantenerla el SGSISD; estando alineada con los objetivos estratégicos, la misión, la visión de la entidad y la ley.</p> <p>Incluirá los objetivos de seguridad de la información, los estándares o marco de referencia en que se basa el SGSISD y su compromiso para cumplir con los requisitos que se adopten de los mismos.</p>
	Requisitos (Guía de implementación ISO/IEC 27002:2015)	N.A.
	Requisitos de cumplimiento	a) 6.2. ISO/IEC 27001:2013 b) 07. Planificación, Anexo 1 del MSPI del MinTIC
	Procesos propietarios	1. Planeación Estratégica 2. Gestión TIC
B. Política de control de acceso, uso de redes y servicios de red	Descripción	Establecer, documentar y revisar una política de control de acceso a acorde con las necesidades de la entidad en SI.
	Contenido (Guía de implementación ISO/IEC 27002:2015)	<ul style="list-style-type: none"> A) Requisitos de seguridad para los sistemas de información misionales y activos críticos. B) Reglas de divulgación y autorización de la información. C) Coherencia entre los derechos de acceso y las políticas de clasificación de la información en los sistemas y redes. D) Coherencia con la legislación pertinente y los acuerdos contractuales. E) Derechos de acceso en entornos distribuidos y de red. F) Segregación de los roles de control de acceso. G) Requisitos para la autorización formal de las solicitudes de acceso. H) Requisitos para la revisión periódica de derechos de acceso. I) Retiro de derechos de acceso. J) Custodia de los registros de los eventos significativos de uso y gestión de identificación de usuarios, e información secreta para la autenticación. K) Roles de acceso privilegiado. L) Accesos a uso de redes y servicios de red. M) Procedimientos de autorización para el uso de redes y servicios de red. N) Controles y procedimientos para proteger el acceso a las conexiones de red y a los servicios de red. O) Medios usados y aprobados para acceder a las redes y a los servicios de red. P) Monitoreo del uso de los servicios de red. Q) Requisitos de autenticación de usuarios para acceder a los servicios de red. <p>- Los propietarios de los activos deben definir los usuarios autorizados para el uso de la información y las reglas y restricciones de acceso.</p> <p>- Los controles de acceso a la información serán tanto lógicos como físicos.</p>

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 102 de 111


	Controles asociados	Relacionados: A.9.1.1; A.9.1.2; A.8.1.2; A.8.2.2; A.18.1.1; A.9.2.1; A.9.2.2; A.9.2.6; A.9.2.3. Deben implementarse coherentes o alineados con la política: A.8.1.2; A.8.2.1; A.9.1.2; A.9.2.3; A.9.4.1; A.9.4.2; A.13.1.3;
	Procesos propietarios	1. Gestión TIC
C. Directrices de clasificación de la información	Descripción	Describe la forma de clasificación, identificación y almacenamiento de la información y sus activos asociados.
	Contenido (Guía de implementación ISO/IEC 27002:2015)	<ul style="list-style-type: none"> A) Definición del esquema de clasificación de activos. B) Los activos de diferente información se deben clasificar de conformidad con la clasificación de la información que se almacena, maneja, proceso o protege el activo. C) El nivel de protección del esquema se establecerá teniendo en cuenta la confidencialidad, integridad y disponibilidad de la información y cualquier otro requisito que la información requiera. D) La entidad debe clasificar la información y los activos conforme al esquema establecido. E) La clasificación de los activos debe poder identificar el proceso y el área a la que pertenecen. F) El esquema de clasificación debe poder indicar el valor de los activos dada su sensibilidad y criticidad. G) El esquema de clasificación de la confidencialidad de la información debe cumplir con las leyes de Transparencia y Acceso a la Información Pública, y de Protección de Datos Personales; porque, se implementará el modelo de identificación de activos de información de la Guía 11.3. "Gestión de inventario y clasificación de activos e infraestructura crítica" del Anexo 1 del MSPI del MinTIC, V4.0. H) Un etiquetado de la información que abarque la información y sus activos relacionados en formatos físicos y electrónicos. I) Restricciones de acceso que soporten los requisitos de protección para cada nivel de clasificación. J) Almacenamiento de los activos de acuerdo con su naturaleza y las especificaciones del fabricante. K) Establecer quienes son los receptores autorizados de la información.
	Controles asociados	Relacionados: A.8.2.1; A.8.2.2; A.8.2.3. Deben implementarse coherentes o alineados con la directriz: A.9.1.1; A.11.2.9; A.13.2.2; A.14.1.1; A.15.1.2.
	Procesos propietarios	<ul style="list-style-type: none"> 1. Mejora Continua 2. Planeación Estratégica 3. Gestión Documental 4. Investigación y Judicialización (Bodegas de evidencia)
	Descripción	Establece los lineamientos para prevenir el acceso físico no autorizado y la violación de la seguridad física de la información.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 103 de 111


D. Directrices de seguridad física y de entorno	Contenido (Guía de implementación ISO/IEC 27002:2015)	<ul style="list-style-type: none"> A) Reglas para establecer el área de procesamiento de información, los perímetros de seguridad y la ubicación. B) Identificación de riesgos de seguridad física y de entorno, y que se debe hacer o como se deben mejorar los resultados de su valoración. C) Definir estándares de seguridad para las áreas de procesamiento de información. D) Control de acceso para las áreas de procesamiento y almacenamiento de información. E) Asignación de recursos para la seguridad física de la información. F) Implementación de áreas seguras para el manejo, procesamiento y almacenamiento de información crítica. G) Reglas de autorización para el retiro o uso de equipos o de información fuera del perímetro de seguridad. H) Disposición segura o reutilización de equipos. I) Requisitos de seguridad para proteger los equipos desatendidos.
	Controles asociados	Relacionados: A.11.1.1; A.11.1.2; A.11.1.3; A.11.1.4; A.11.1.5; A.11.1.6; A.11.2.1; A.11.2.2; A.11.2.3; A.11.2.4; A.11.2.5; A.11.2.6; A.11.2.7; A.11.2.8. Deben implementarse coherentes o alineados con la directriz: 12.1.1.
	Procesos propietarios	<ul style="list-style-type: none"> 1. Gestión TIC 2. Gestión Documental 3. Gestión de Bienes 4. Investigación y Judicialización (Bodegas de evidencia)
E. Directrices para el uso aceptable de activos	Descripción	Identificación de las reglas para el uso aceptable de la información, sus de los activos de información y las áreas de procesamiento de información.
	Contenido (Guía de implementación ISO/IEC 27002:2015)	<ul style="list-style-type: none"> A) Toma de conciencia de los requisitos de seguridad de la información. B) Responsabilidades para el uso de los activos de información y de las áreas de procesamiento y almacenamiento de información.
	Controles asociados	Relacionados: A.8.1.3.
	Procesos propietarios	<ul style="list-style-type: none"> 1. Gestión TIC 2. Planeación Estratégica 3. Gestión Documental 4. Investigación y Judicialización (Bodegas de evidencia)
F. Política de escritorio y pantalla limpios	Descripción	Definición de reglas de escritorio limpio para los papeles y medios de almacenamiento removibles y las de pantalla limpia para los equipo y áreas de procesamiento de información, con el fin de reducir los riesgos de acceso no autorizado, pérdida o daño de información, durante o por fuera del horario laboral.
	Contenido (Guía de implementación ISO/IEC 27002:2015)	<ul style="list-style-type: none"> A) Debe tener en cuenta las clasificaciones de la información, para establecer qué tipo de información (crítica), no puede estar descuidada. B) Establecer deberes y responsabilidades sobre la información con permiso de uso o custodia para un servidor. C) Toma de conciencia sobre la seguridad de la información a cargo. D) Reglas de almacenamiento de la información sensible o clasificada (crítica) física, ya sea que su medio de almacenamiento sea papel o electrónico. E) Reglas de protección para equipos desatendidos. F) Uso autorizado de medios de copiado (cámaras, scanner, fotocopadoras, fax). G) Protección de medios que contengan información sensible o clasificada (crítica). H) Tener en cuenta para la política, requisitos legales, contractuales, riesgos y culturales de la entidad.
	Controles asociados	Relacionados: A.11.2.9 - A.8.2.1; A.8.2.2; A.8.2.3; A.18.1.1; A.18.1.2; A.18.1.3; A.18.1.4; A.18.1.5. Deben implementarse coherentes o alineados con la política: A.11.2.6.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 104 de 111


	Procesos propietarios	<ol style="list-style-type: none"> 1. Mejora Continua 2. Planeación Estratégica
G. Política de transferencia de información y seguridad de las comunicaciones	Descripción	Desarrollar los lineamientos para la estandarización de la seguridad de la información en las comunicaciones y en los procesos de transferencia de información dentro de la entidad y con terceros.
	Contenido (Guía de implementación ISO/IEC 27002:2015)	<ol style="list-style-type: none"> A) Definir un procedimiento que establezca las actividades a realizar para definir qué información se va a transferir en cada caso, qué características tiene la información, las obligaciones o compromisos de ley, contractuales o acuerdos gubernamentales que soportan la transferencia o la compartición de la información. Además de cuál es el medio idóneo para transferir la información reglas las características de cada caso. B) Diseño de procedimientos para proteger la información transferida contra enrutamiento, interceptación, destrucción, copiado y modificación. C) Permisos de uso aceptable para el receptor, definido por el propietario de la información. D) Procedimientos y lineamientos para la detección de software malicioso y la protección contra éste. E) Protocolos y procedimientos para la protección de información sensible comunicada que este en formatos adjuntos. F) Políticas o lineamientos para el uso aceptable de las instalaciones de comunicación. G) Uso responsable de las comunicaciones y consecuencias por usos inadecuados como: cadenas, difamación, acoso, suplantación, compras no autorizadas, etc. Se deben definir cuáles son los usos no autorizados, partiendo de la premisa de definir primero los usos autorizados y lo que no esté dentro de lo autorizado se entiendo por no autorizado. H) Uso de técnicas criptográficas para proteger la integridad, confidencialidad y autenticidad de la información. I) Directrices para la retención y disposición de la correspondencia, incluidos los mensajes. J) Controles y restricciones asociados con las instalaciones de comunicaciones. K) Concientización y sensibilización al personal y a todos los que intervienen el proceso de comunicaciones y transmisión de la información, de no revelar información confidencial o sensible. L) Contemplar dentro de la política cualquier tipo de medio posible para la transmisión de la información como: red, interfaces, webservices con externos, correos (físicos y electrónicos), mensajes, fax, conversaciones, video, videoconferencia, etc. M) Procedimiento y lineamientos para asegurar trazabilidad, no repudio, entre otros. N) Acuerdos y lineamientos de mensajería. O) Acuerdos de confidencialidad en todos los procesos que se requieran para prevenir las violaciones a la seguridad de la información.
	Controles asociados	Relacionados: A.13.1.1; A.13.1.2; A.13.1.3; A.13.2.1; 13.2.2; A.13.2.3; A.13.2.4. Deben implementarse coherentes o alineados con la política: A.7.1.2; A.7.3.1; A.9.2.2; A.12.6.1.
	Procesos propietarios	<ol style="list-style-type: none"> 1. Gestión TIC 2. Planeación Estratégica
H. Política de dispositivos móviles y teletrabajo	Descripción	Definir las reglas y lineamientos para la seguridad de la información en la modalidad de teletrabajo y trabajo en casa, y cuando hay manejo de información desde dispositivos móviles.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 105 de 111


	Contenido (Guía de implementación ISO/IEC 27002:2015)	<ul style="list-style-type: none"> A) Definir la modalidad de teletrabajo y trabajo en casa diferenciando cada una, tener en cuenta los riesgos de seguridad de la información cuando se trabaja en entornos no seguros o fuera de las instalaciones protegidas. B) Definir las condiciones y restricciones del teletrabajo o trabajo en casa en cuanto a: seguridad física (edificación, entorno local, etc., cuando aplique), requisitos de seguridad de las comunicaciones (internet, red), requisitos de seguridad del software. C) Suministro de acceso a escritorio virtual desde un equipo persona y almacenamiento en éste. D) Reglas y lineamientos para minimizar o controlar amenaza de acceso no autorizado a información o recurso por parte de personas no autorizadas del entorno de trabajo que usan el mismo equipo personal (familiares, amigos, etc.) E) Uso de redes domésticas y requisitos de configuración permitidos. F) Lineamientos, políticas o procedimientos para aclarar conflictos de propiedad intelectual por desarrollo efectuados en equipos de propiedad privada. G) Licenciamiento y requisitos de software, firewall y antivirus. H) Revisiones de configuración segura y cumplimiento de requisitos en equipo destinados a teletrabajo o trabajo en casa, tener en cuenta restricciones de ley para revisión en equipos de propiedad privada. I) Otras de competencia de talento humano como: horario de trabajo, clasificación de la información que puede mantener, servicios que puede prestar, sistemas a los que puede acceder, mobiliario, etc. Lo anterior se debe evaluar en los dos escenarios, cuando la entidad da los suministros y cuando son de propiedad privada, sobre los cuales no tiene gobernabilidad la Entidad, pero pueden generar vulnerabilidades para la seguridad de la información, en los dos casos, que reglas, compromiso y deberes se deben cumplir por parte de los servidores para generar seguridad para la entidad. J) Crear acuerdo de confidencialidad según la función, el acceso a información crítica o sensible y el proceso al que pertenece, tanto para teletrabajo y trabajo en casa.
--	--	---

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 106 de 111


		<p>K) Se tendrá en cuenta los riesgos de trabajar con dispositivos móviles en entornos no protegidos.</p> <p>L) Desarrollará las reglas y responsabilidades del personal que trabaja con dispositivos móviles ya sea interno o externo, desde que manejen información sensible o crítica en los dispositivos.</p> <p>M) Se considerarán los registros de los dispositivos móviles y los requisitos de protección física cuando estos son asignados por la entidad (contra robo, contra daño), o cuando son susceptibles a extracción de información sensible o crítica no autorizada por medio de dispositivos externos como USB (aplica para dispositivos móviles de usos personal o institucional).</p> <p>N) Restricciones y requisitos para la instalación de software, parches y actualizaciones en dispositivos móviles de la entidad y reglas preventivas de riesgos por instalación de software para los personales que manejen información sensible o crítica.</p> <p>O) A tener en consideración según las necesidades y requisitos de la entidad: controles de acceso, técnicas criptográficas, control contra software maliciosos, deshabilitación remota, borrado y cierre, copias de respaldo y uso de servicios y aplicaciones web.</p> <p>P) Entrenamiento y concientización sobre las responsabilidades, riesgo y políticas de seguridad de la información para el uso de dispositivos móviles, para el personal que usa éstos como parte de sus herramientas de trabajo.</p> <p>Q) Definir si se permiten o no el uso de dispositivos móviles personales para el manejo de información crítica o sensible o trabajo de la entidad, y las reglas de uso para la separación entre lo privado y la correspondiente a la entidad, incluido el uso del software para la separación de uso y proteger los todos de la entidad.</p> <p>R) Diseñar un acuerdo de confidencialidad para el uso de dispositivos móviles, contemplar los dos escenarios de uso privado e institucional, en donde los servidores o personal autorizado, reconocen sus deberes, responsabilidades, consecuencias y limitaciones de uso.</p> <p>S) Contemplar todos los posibles controles de seguridad de la información como por ejemplo para trabajo en red, correo electrónico, acceso a internet, manejo de archivos, acceso remoto, etc.</p> <p>T) Otros para tener en cuenta para teletrabajo, trabajo en casa y uso de dispositivos móviles: mantenimiento de hardware y software, seguros, reglas para copias de respaldo y continuidad de negocio, auditoría y seguimiento, revocación de permisos, devolución de equipos, etc.</p>
	Controles asociados	Relacionados: A.6.2.1; A.6.2.2; A.9.2.4; A.10.1.1 y siguientes del 10; A.18.1.1. Deben implementarse coherentes o alineados con la política: A.18.1.1.
	Procesos propietarios	<ol style="list-style-type: none"> 1. Gestión TIC 2. Planeación Estratégica 3. Gestión de Bienes 4. Gestión del Talento Humano
	Descripción	Establecer las restricciones para el uso y la instalación de software en la entidad.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 107 de 111


I. Política de prohibición de uso e instalación de software no autorizado	Contenido (Guía de implementación ISO/IEC 27002:2015)	<ul style="list-style-type: none"> A) Definir listas negras y listas blancas para uso de software en la entidad, todo lo que no esté en las listas blancas se asume como software prohibido, y cuales con los requisitos para los softwares aprobados. B) Definir un procedimiento de respuesta a incidentes para la instalación de software y para la aprobación de aquellos que según el usuario se requieren, pero no están en la lista blanca. C) Las listas blancas estarán separadas por software aprobadas por proceso y generales aprobados para toda la entidad. D) Hacer toma de conciencia sobre la vulnerabilidad que trae a la seguridad de la información las instalaciones de software no autorizados y no vigilados. E) Desarrollar un proceso de vulnerabilidades técnicas alineado con la respuesta a incidentes. F) La instalación de software será exclusiva de la SubTIC o de quienes ellos les deleguen o autoricen esta función, y estará incluido dentro de un procedimiento. G) Los procesos que instalen software por fuera de la gobernabilidad de SubTIC, deberán garantizar la seguridad de la información y responder por amenazas y vulnerabilidades; si SubTIC no autoriza o no responde por este software, se evaluará la posibilidad de que estén por fuera de la red y de los equipos de la entidad y de igual manera asegurar y responder por la seguridad de información que manejan estos activos, así como declararlos en el inventario. De lo contrario se debe prohibir su instalación. H) Aplicar el principio de menor privilegio para el manejo de software a personal no autorizado. Los privilegios se deben conceder con relación a los roles de los usuarios. I) En todos los casos, los softwares utilitarios solo pueden ser usados por SubTIC y se deben definir cuáles son los autorizados, en donde y en qué actividades se pueden usar. J) Restringir en cualquier circunstancia el uso de software no licenciado y libre, solo bajo la autorización y responsabilidad SubTIC de podrán instalar, la solicitud de instalación de este tipo de software deberá estar justificada por el proceso. K) Se definirán controles lógicos para evitar la instalación de softwares no autorizados.
	Controles asociados	Relacionados: A.12.2.1; A.12.6.1; A.12.6.2. Deben implementarse coherentes o alineados con la política: A.14.2.4; A.12.5.1.
	Procesos propietarios	1. SubTIC
J. Política de copias de respaldo	Descripción	Establecer las reglas y requisitos para la realización de las copias de respaldo.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 108 de 111


	Contenido (Guía de implementación ISO/IEC 27002:2015)	<ul style="list-style-type: none"> A) Definir las reglas y los requisitos para las copias de respaldo de la información, software y sistemas. B) Definir requisitos de retención y protección. C) Tener en cuenta la gestión de los riesgos para la recuperación después de desastres o fallas del medio. D) Diseñar un plan de copias de respaldo que contemple: <p>13. Producir registros exactos y completos de las copias de respaldo y procedimientos de restauración.</p> <p>14. Definir requisitos, alcance y frecuencia para las copias de respaldo, teniendo en cuenta la seguridad de la información, la criticidad de los activos y las necesidades de la entidad.</p> <p>15. Tener en cuenta todos los riesgos de seguridad de la información que pueden sufrir las copias de respaldo y controlarlos.</p> <p>16. Tener en cuenta los requisitos de continuidad de negocio.</p> <ul style="list-style-type: none"> E) Definir las reglas y deberes de los servidores con respecto al respaldo de la información de su propiedad (la que producen) y la actualización de los sistemas. F) Generar conciencia y compromiso acerca de la gestión de copias de respaldo, así como las consecuencias y responsabilidades, y la seguridad que se debe tener con las mismas al exponer la información respaldada a vulnerabilidades y amenazas.
	Controles asociados	Relacionados: A.12.3.1. Deben implementarse coherentes o alineados con la política: N.A.
	Procesos propietarios	<ul style="list-style-type: none"> 1. Gestión TIC 2. Gestión Documental
K. Política de controles criptográficos, uso, protección y tiempo de vida de las llaves criptográficas	Descripción	Desarrollar controles para asegurar la confidencialidad, integridad o autenticidad, autenticación y no-repudio de la información crítica o sensible ya sea almacenada o transmitida.
	Contenido (Guía de implementación ISO/IEC 27002:2015)	<ul style="list-style-type: none"> A) Enfoque de la alta dirección con respecto al uso de controles criptográficos. B) Principios sobre los cuales se debería proteger la información de la entidad. C) Tener en cuenta la valoración de los riesgos para determinar el nivel de protección que se quiere. D) Incluir cifrado, según los requisitos de ley y las necesidades de la entidad, para los dispositivos móviles, removibles y líneas de comunicación. E) Métodos para la gestión, protección llaves criptográficas y la recuperación de la información cuando éstas estén comprometidas. F) Roles y responsabilidades. G) Normas por adoptar para la implementación efectiva en toda la entidad. H) Impacto en los controles que dependas de la inspección de contenido. I) Ajustar a los requisitos permitidos por la ley el uso de controles criptográficos. J) Definir reglas para la transferencia de información con controles criptográficos.
	Controles asociados	Relacionados: A.10.1.1; A.10.1.2; A.18.1.5. Deben implementarse coherentes o alineados con la política: A.10.1.2; A.18.1.5.
	Procesos propietarios	<ul style="list-style-type: none"> 1. Gestión TIC
L. Directrices de privacidad y protección de la información de datos personales	Descripción	Establecer los lineamientos para asegurar la privacidad y protección de los datos personales
	Contenido (Guía de implementación ISO/IEC 27002:2015)	Se debe definir la política de privacidad y protección de la información de datos personales de la FGN en función de la Ley 1581 de 2012.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 109 de 111

	Controles asociados	Relacionados: A.18.1.4. Deben implementarse coherentes o alineados con la directriz: A.18.1.5; A.7.1.2; A.12.4.1.
	Procesos propietarios	<ol style="list-style-type: none"> 1. Gestión Documental 2. Gestión TIC 3. Planeación Estratégica
M. Política de seguridad de la información en la relación con los proveedores	Descripción	Definir las reglas, requisitos, deberes y responsabilidades en la relación con proveedores para la seguridad de la información de la entidad.
	Contenido (Guía de implementación ISO/IEC 27002:2015)	<ol style="list-style-type: none"> A) Identificar los tipos o grupos de proveedores a los que se les permite el acceso a la información, como: servicios de TÍ, consultoría y asesoría, servicios tercerizados, etc. B) Identificar los tipos o grupos de proveedores a los que no se le permite acceso a la información, como: abastecimiento de suministro o almacenes, obre civil. Sin embargo, esto deberán tener otro tipo de deberes y responsabilidades de no divulgación de información. C) Establecer los permisos de acceso a la información para los proveedores, según las reglas que tenga cada proceso, sistema o servicio, y conforme a los lineamientos y autorizaciones de los propietarios de la información y custodios funcionales y técnicos. D) Establecer a qué tipo de información, no podrían tener acceso los proveedores y en caso de requerirse, quien sería el responsable de autorizarlo. Siempre se debe tener la autorización del propietario de la información para permitir el acceso a un tercero. E) Requisitos que deben cumplir los proveedores para poder emitir la autorización de acceso a información, los mismos deben estar diferenciados por el tipo de proveedor y el nivel de acceso a la información. F) Formato de confidencialidad en donde se especifiquen deberes, responsabilidades y restricciones, según el tipo de acceso otorgado, los riesgos de la información a acceder y la reglamentación existente para: cada tipo de información, activo de información o área de procesamiento de información. G) Actividades normalizadas para la gestión de relaciones con proveedores, se deben identificar los pasos a seguir en caso de violación de seguridad de la información por parte de un proveedor y que acciones se deben tomar según el nivel de riesgo y la criticidad o sensibilidad de la información. H) Procedimiento de seguimiento al cumplimiento de los requisitos de seguridad de la información para cada tipo de proveedor y tipo de acceso, incluida, de ser necesario, la revisión por una tercera parte y la validación del producto. Se deben contemplar todos los permisos otorgados de acceso a la información (físicos o informáticos), acceso a áreas de procesamiento de información, etc. I) Tipo de obligaciones aplicables a los proveedores para proteger la información de la entidad en todas las etapas de la contratación, precontractual, contractual y poscontractual. J) Manejo de incidentes de seguridad de la información asociados con el acceso a proveedores. K) Toma de conciencia del personal que tendrá trato con el proveedor con respecto a la seguridad de la información, el nivel de acceso otorgado al proveedor, incluidas las responsabilidades y restricciones de los servidores, la entidad y el proveedor. L) Planes de contingencia y de continuidad del negocio. M) Acuerdos de acceso a la información firmados por ambas partes. N) Actividades de transición en la entrega de información a la tuvo acceso o conservo el proveedor, acuerdos de custodia o borrado de la misma.
	Controles asociados	Relacionados: A.15.1.1; Deben implementarse coherentes o alineados con la política: N.A.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 110 de 111

	Procesos propietarios	<ol style="list-style-type: none"> 1. Gestión Contractual 2. Gestión TIC 3. Gestión Documental
N. Directrices de retención de registros	Descripción	Asegurar la adecuada recolección de registros después de un evento de seguridad de la información.
	Contenido (Guía de implementación ISO/IEC 27002:2015)	<ol style="list-style-type: none"> A) Definir procedimientos para la identificación, recolección y preservación de evidencia cuando se violen o vulnere la seguridad de la información de la entidad y se requiera continuar con acciones legales o disciplinarias. B) Para tener en cuenta: cadena de custodia, seguridad de la evidencia y del personal, apertura de investigación formal y no formal, compulsas de copias, etc. C) Se debe contar con la participación del área de criminalista de la entidad.
	Controles asociados	Relacionados: A.16.1.7. Deben implementarse coherentes o alineados con la directriz: A.7.2.3; A.12.4.2; A.16.1.5.
	Procesos propietarios	<ol style="list-style-type: none"> 1. Investigación y Judicialización 2. Planeación Estratégica 3. Gestión TIC 4. Gestión Documental
O. Política de desarrollo seguro	Descripción	Establecer las normas y lineamientos para el desarrollo seguro de software, servicios, aplicaciones, sistemas en la entidad.
	Contenido (Guía de implementación ISO/IEC 27002:2015)	<p>El desarrollo seguro es un requisito para crear un servicio, arquitectura, software o sistema seguros. Para el desarrollo seguro se deben considerar:</p> <ol style="list-style-type: none"> A) Ambiente de desarrollo. B) Seguridad en la metodología de desarrollo y directrices de codificación segura para cada lenguaje de programación usado, en el ciclo de vida de desarrollo de software. C) Requisitos de seguridad en la fase de diseño D) Puntos de control de seguridad dentro de los hitos. del proyecto. E) Depósitos seguros. F) Seguridad en el control de la versión. G) conocimiento requerido sobre la seguridad de la aplicación. H) Capacidad de los desarrolladores para evitar, encontrar y resolver las vulnerabilidades. I) Técnicas de programación segura para desarrollo nuevo como para reúso de código. J) Exigir estándares de codificación donde sea pertinente. K) Formar a los desarrolladores en uso y prueba. K) Los softwares desarrollados externamente deberán contar con estándares certificados de desarrollo seguro, conocer las políticas y lineamientos del SGSISD de la entidad aplicándolos cuando sea requerido.
	Controles asociados	Relacionados: A.14.2.1; A.14.2.7. Deben implementarse coherentes o alineados con la política: A.14.2.9; A.14.2.7; A.12.1.4.
	Procesos propietarios	<ol style="list-style-type: none"> 1. Gestión TIC
P. Directrices para la protección de la propiedad intelectual	Descripción	Establecer e implementar las directrices para la protección de la propiedad intelectual
	Contenido (Guía de implementación ISO/IEC 27002:2015)	<p>Las cuales deben incluir:</p> <ol style="list-style-type: none"> A) El Cumplimiento de los derechos de propiedad intelectual que defina el uso legal del software y de productos informáticos.

	PROCESO PLANEACIÓN ESTRATÉGICA	Código: FGN-EP01-M-02
	MANUAL DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL DE LA FGN - SGSISD	Versión: 01 Página: 111 de 111

		<p>B) La adquisición de software solo se hará por los medios establecidos por el proceso de Gestión Contractual, con el fin de asegurar la adquisición de proveedores aprobados, conocidos y confiables que no incurran en la violación de derechos de autor.</p> <p>C) La reglamentar de las donaciones de software y productos informáticos.</p> <p>D) Mantener la conciencia en los servidores de las directrices de propiedad intelectual y las sanciones disciplinarias que se podrían originar por su incumplimiento.</p> <p>E) Mantener el inventario de activos actualizado e identificar en éstos los requisitos para la protección de la propiedad intelectual.</p> <p>F) Mantener de cada activo relacionado en el inventario (si aplica por su naturaleza), la evidencia de la propiedad intelectual como licencias, discos maestros, manuales, etc.</p> <p>G) Implementar controles para asegurar que no se exceda el número máximo de usuarios permitidos dentro de las licencias.</p> <p>H) Realizar seguimiento y controlar que en los equipos propiedad de la entidad solo se instales software autorizados y productos con licencia (ver 8.1.1. y 8.1.4.)</p> <p>I) Mantener las condiciones de licenciamiento apropiadas para cada software.</p> <p>J) Generar lineamientos o actividades documentadas para la disposición o transferencia de software a otros, o la recepción desde entidades externas.</p> <p>K) Cumplir los términos y condiciones de cada software y la información obtenida de las redes públicas.</p> <p>L) Vigilar que no se incurra en faltas contra los derechos de autor o contra la ley al duplicar, convertir a otro formato, transformar o extraer de registro comerciales (video o audio). Quedan excluidos con forme lo permitan el Código Penal Colombiano y la Ley, aquellos que se usen dentro de cualquier etapa o actividad del proceso de penal, según lo definan los procesos misionales.</p> <p>M) No copiar total ni parcialmente libros, artículos, reportajes u otros documentos diferentes a los permitidos por la ley de derechos de autor o sin citar la referencia.</p> <p>Nota. Según la <u>información adicional</u> del numeral 18.1.2 de la ISO/IEC 27002:2015 ..."<i>Los derechos de propiedad intelectual incluyen derechos de autor de software o de documentos, derechos de diseño, marcas registradas, patentes y licencias de códigos fuentes.</i>" ...</p>
	Controles asociados	Relacionados: A.18.1.2. Deben implementarse coherentes o alineados con la directriz: A.7.1.2; A.14.2.7.
	Procesos propietarios	<ol style="list-style-type: none"> 1. Gestión TIC 2. Planeación Estratégica 3. Gestión Documental 4. Gestión Jurídica
Q. Política de integridad de la información	Descripción	Establecer e implementar la política de integridad de la información de la FGN
	Contenido (MSPI del MinTIC)	Modelo de Seguridad y Privacidad de la Información MSPSI del MinTIC
	Controles y requisitos asociados	Relacionados: A.11.2.4; 6.1.2 y 6.1.3. Deben implementarse coherentes o alineados con los marcos de referencia: ISO/IEC 27005:2020 y Anexo 4 MGRSD.
	Procesos propietarios	<ul style="list-style-type: none"> ▪ Gestión TIC ▪ Planeación Estratégica ▪ Gestión Jurídica ▪ Planeación Estratégica