PROPÓSITO

Garantizar que el sistema de seguridad de la información para la Unidad Nacional de Protección- UNP se establezca, con el fin de cumplir con los requisitos de seguridad, definidos en un Sistema de Gestión de la Seguridad de la Información -SGSI y el Modelo de seguridad y privacidad de la información- MSPI, que ayudarán, mediante su implementación, a preservar la confidencialidad, integridad y disponibilidad de la información en la Entidad, en el cual se implementaran los controles, procedimientos y estándares definidos.

ALCANCE

El procedimiento inicia con la sensibilización al talento humano de la Entidad en temas del manejo de seguridad de la información, en los cuales se deberá cubrir los aspectos administrativos o que hagan referencia al modelo de seguridad y privacidad de la información MSPI y finaliza con el control de la información institucional generada por cada Coordinación. El procedimiento aplica a toda la Unidad Nacional de Protección, incluyendo a todos los funcionarios, contratistas y terceros.

RESPONSABILIDADES

RESPONSABLES	RESPONSABILIDADES
Grupo Oficina Asesora de Planeación e Información	1. Coordina el desarrollo e implantación del Modelo de Seguridad y Privacidad de la Información -MSPI, en lo que respecta como oficina asesora de la dirección, a aconsejar y liderar ante la dirección el gobierno de TI y de seguridad de la Información de la Entidad. 2. Gestiona ante dirección el desarrollo, firma, promulgación, uso y apropiación de la Política de alto nivel denominada Política General de Seguridad de la Información. 3. Lidera junto con el responsable y el Oficial de Seguridad de la Información el Comité de Seguridad de la Información o el que haga sus veces.
Secretaria General	1. Gestiona la disponibilidad administrativa y de recursos para asumir la operación de seguridad de la información de la Entidad en el sentido de que se necesita de recursos humanos, técnicos, administrativos y financieros para su operación.
Coordinador de Talento Humano	1. Dirige y coordina la implementación del plan de capacitación, la política de tratamiento de datos personales y el acuerdo de confidencialidad de funcionarios, contratistas y terceros de la UNP.
Lider y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información.	1. Coordina y dispone junto con el oficial de seguridad de la información las medidas tecnológicas para el aseguramiento de la seguridad informática y de la información. 2. Establece una configuración de acceso a la información adecuada, para cada uno de los servidores públicos, proveedores y partes interesadas, que requieran acceder los sistemas de información y recursos informáticos de la Entidad.
Oficial de seguridad de información	1. Coordina y dispone junto con el oficial de seguridad de la información las medidas tecnológicas para el aseguramiento de la seguridad informática y de la información. 2. Articula los procesos y procedimientos de seguridad de la información y velar por su cumplimiento. 3. Articula la estrategia de seguridad de la información de la Entidad de acuerdo a la política nacional emitida por MinTIC de gobierno

	digital y a su componente el modelo de seguridad y privacidad de la información, denominado MSPI. Actualiza y presenta ante el coordinador de las Políticas de Seguridad de la Información, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente. 4. Verifica el cumplimiento de las políticas de seguridad de la información aquí mencionadas.
Funcionarios, Contratistas y terceros.	1. Responsable del manejo seguro de la información y propietario de la misma.

DEFINICIONES	
TERMINO	**DEFINICIÓN**
Activo de Información	La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la Entidad y, en consecuencia, necesita una protección adecuada.
Amenaza informática	La aparición de una situación potencial o actual donde una persona tiene la capacidad de generar una agresión cibernética contra la población, el territorio, la organización política del Estado (Ministerio de Defensa de Colombia).
Clasificación de la Información	Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado6.
Confidencialidad	La propiedad de la información de no ponerse a disposición o ser revelada a individuos, Entidades o procesos no autorizados.
Custodia de la información	Es una parte designada de la organización, 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, con base en los controles de seguridad existentes en la Entidad.
Datos personales sensibles	Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.
Incidente de seguridad de la información	Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Información	Datos relacionados que tienen significado para la Entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la Entidad y, en consecuencia, necesita una protección adecuada.
Modelo de seguridad y privacidad de la información- MSPI	Es una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente “Seguridad y Privacidad de la Información”. Fue creada por el Ministerio de Tecnologías de

	la Información y las Comunicaciones con uso libre sin fines lucrativos, por esta razón se prohíbe la comercialización y explotación de la misma.
Propietario de la información	Es la persona que crea un activo de información y por ende tiene la facultad de definir su clasificación y los derechos de acceso que tienen los demás usuarios.
Frequently asked questions –FAQ's	El término preguntas frecuentes (traducción al español de la expresión inglesa Frequently Asked Questions, cuyo acrónimo es FAQ) se refiere a una lista de preguntas y respuestas que surgen frecuentemente dentro de un determinado contexto y para un tema en particular.
Recursos tecnológicos	Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento.
TI	Tecnologías de Información
Vulnerabilidades	Son las debilidades, hoyos de seguridad o falencias inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por las amenazas, las cuales se constituyen en fuentes de riesgo.

MARCO LEGAL

- ✓ **Ley 527 de 1999**. *"Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las Entidades de certificación y se dictan otras disposiciones".*
- ✓ **Ley 1150 de 2007.** *"Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con recursos públicos"*
- ✓ **Ley 1273 de 2009**. *"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".*
- ✓ **Ley 1581 de 2012.** *"Por la cual se dictan disposiciones generales para la protección de datos personales".*
- ✓ **Decreto 2573 de 2014**. *"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".*
- ✓ **Decreto 1008 de 2018.** *"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".*
- ✓ **CONPES 3701 de 2011**.Lineamientos de Política para Ciber-seguridad y Ciber-defensa
- ✓ **CONPES 3854 de 2016**. Política Nacional de Seguridad digital.

CONSIDERACIONES GENERALES

1. El sistema de Seguridad de la Información debe ser alineado con al Modelo de Seguridad y Privacidad de la Información establecido por el MinTIC y este a la vez se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia de Gobierno Digital.
2. El marco de referencia para el desarrollo del presente procedimiento se realiza con base los siguientes documentos emitidos por Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC:
    - La Guía de seguridad y privacidad de la información.
    - Guía para la Gestión y Clasificación de Activos de Información.

DESCRIPCIÓN DEL PROCEDIMIENTO			
RESPONSABLE	**ACTIVIDAD**	**DESCRIPCIÓN DE LA ACTIVIDAD**	**REGSITRO Y PUNTOS DE CONTROL**
a). Seguridad del recurso humano			
Lider y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información. Coordinación Talento Humano	1. Diseñar plan de sensibilización en seguridad de la información.	Este plan se desarrolla a partir de las políticas del modelo de seguridad y privacidad de la información del MINTIC, también se realiza un diagnóstico de las necesidades de sensibilización a nivel institucional durante las etapas de vinculación laboral, en el ejercicio de la labor y en el proceso de desvinculación.	**Registro:** Plan de sensibilización en seguridad de la información.
Lider y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información. Coordinación Talento Humano. Oficina de comunicaciones	2. Ejecutar el plan de sensibilización.	En coordinación con el Grupo de Talento Humano y la oficina de Comunicaciones estratégicas se ejecuta el plan de sensibilización, teniendo en cuenta el diagnostico detectado en la fase inicial, se establece los medios de divulgación que estén disponibles en la Entidad.	**Registro:** Cronograma del plan de sensibilización. Formato SGI-FT-03 Listado de asistencia.
Lider y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información. Coordinación Talento Humano.	3. Evaluar plan de sensibilización	Al finalizar el desarrollo de talleres, se realiza encuestas de satisfacción y evaluación de conocimientos generales.	**Registro:** Formato GTH-FT-28 Evaluación actividades de capacitación.
b). Control acceso			
Lider y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información.	1. Diseñar la política de acceso a los sistemas de información y definir permisos de acceso a los	Se diseña la política de acceso a los sistemas de información con el objeto de poder definir roles, responsabilidades y permisos a los servicios y sistemas de información que tenga acceso de acuerdo al rol del funcionario, contratista o tercero de la Entidad.	**Registro:** La política de acceso a los sistemas de información y definir permisos de acceso a los

Oficial de seguridad de la información. Coordinación Talento Humano.	servicios de red.		servicios de red,
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información. Líder del proceso.	2. Definición de roles y permisos de acceso a los servicios y sistemas de información de la Entidad.	Crear la matriz de segregación usuarios y perfiles la cual definirá el tratamiento de los permisos por usuario. La base de datos deberá contener el estado del usuario (Activo o Cancelado). Para la construcción se tiene en cuenta como insumo la base de datos del directorio activo y la información suministrada por los líderes de cada uno de los procesos.	**Registro:** GTE-FT-30 matriz de segregación usuarios y perfiles.
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información	3. Asignar permisos de recursos tecnológicos	Se recepciona el formato modificación o creación de usuario del Líder de cada uno de los procesos de la Entidad del perfil de usuario, bajo el cual se asignan los permisos y accesos a los recursos tecnológicos.	**Registro:** Formato GTE-FT-23 modificación o creación de usuario.
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información.	4. Realizar control de accesos a sistemas, aplicaciones y códigos fuente de programas.	Teniendo en cuenta la política de control de accesos se exige a los usuarios que cumpla las prácticas de la organización para el uso de información y autenticación. Se restringe el acceso a los códigos fuente de los programas. Se verifica periódicamente los controles de acceso, para todos los usuarios incluyendo funcionarios, contratistas, terceros, proveedores y demás partes interesadas, con el fin de revisar que dichos usuarios tengan acceso permitido, únicamente, a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.	**Registro:** Guía para creación de contraseñas seguras.
c). Gestión activos			
Coordinadores de Grupo. Oficial de seguridad de la información	1. Realizar inventario de activos	El inventario de activos de información según el MSPI, debe clasificar los activos de la Unidad Nacional de Protección a los que se les debe brindar mayor protección, pues se debe identificar claramente sus características y rol al interior de los proceso en las áreas de la Entidad. Las actividades por realizar para obtener un inventario de activos son definición, revisión, actualización y publicación, las cuales se deben reflejar documentalmente en la Matriz de Inventario y Clasificación de Activos de Información según el MSPI.	**Registro:** Formato GTE-FT-08 inventario de activos de información
Coordinadores de Grupo.	2. Asignar los activos de información.	La asignación de los activos de la información lo realizará las áreas responsables de cada proceso dentro la Entidad y se publica en el inventario de activos de información de la Entidad.	Registro: Asignación de activos de información

Oficial de seguridad de la información		La Coordinación de seguridad de la Información velara que los activos entregados cumplan con las normas del MSPI.	
Lider y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información.	3. Clasificar la información de gestión de activos	La información debe ser identificada, clasificada y documentada de acuerdo con las guías de Clasificación de la Información establecidas por el MSPI. La Entidad tendrá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad y según el MSPI, y según la guía de Clasificación de la Información para que los propietarios de esta la cataloguen y determinen los controles requeridos para su protección.	**Registro:** Formato GTE-FT-08 inventario activos de información final.
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Propietario de la Información.	4. Etiquetar la información	Para el etiquetado y manipulación de los activos de Información, se tienen en cuenta tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad, según el modelo de la privacidad y seguridad de la información.	**Registro:** Guía para la Gestión y Clasificación de Activos de Información.
Oficial de seguridad de la información.	5. Revisar información	En la actividad de revisión se realizará la verificación que se lleva a cabo para determinar si un activo de información continua o no siendo parte del inventario, o si los valores de evaluación asignados en el inventario y clasificación de activos de Información deben ser modificados.	**Punto de Control:** Verificación de la información en el inventario de activos.
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Coordinación de Grupos	6. Identificar los cambios a realizar al inventario de activos de información.	Una vez se ha definido qué cambios se realizarán en el inventario, desde cada proceso, se procede a actualizar el inventario de activos de información.	**Registro:** Control de cambios al inventario de la información.
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información.	7. Actualizar la matriz de inventario de activos de información.	Todos los activos del inventario se deben identificar de manera adecuada en la matriz de inventario de activos, clasificación y publicación, la cual está conformada de acuerdo al modelo de seguridad y privacidad de la información.	**Registro:** Formato GTE-FT-08 inventario activos de información final.
Oficial de seguridad de la información. Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información.	8. Diseñar la política de gestión de activos	Con la matriz de inventario de activos de información se definirán las reglas generales del uso y gestión de los activos de información y el ciclo de vida de este. La aprobación de la política se realizará a través de la subcomisión de gestión y seguridad de TI.	**Registro:** La política de gestión de activos.

Secretaria General. Jefe de Oficina Asesora de Planeación e Información.			
d). Criptografía			
Oficial de seguridad de la información Grupo de Gestión de las tecnologías de la información	1. Diseñar la política de controles criptográficos.	Diseñar la política de controles criptográficos; Donde se establecen las guías o lineamientos, responsabilidades y procedimientos para realizar los mismos en todas las áreas de la Entidad donde se encuentre información confidencial o clasificada. Para la ejecución de la política de Controles Criptográficos, es necesario tener completada la actividad de gestión de activos de la información. Adicionalmente, se necesita llevar a cabo una tarea de clasificación y etiquetado de la información donde se encuentre identificada la información como confidencial o reservada.	**Registro:** La política de controles criptográficos.
Líder del Grupo de Gestión de las tecnologías de la información. Coordinación de Grupos. Secretaria General. Oficial de seguridad de la información.	2. Ejecutar la política de controles criptográficos	Implementar la política de controles criptográficos en todas las áreas de la Entidad, dependiendo del nivel de clasificación y criticidad de la información. Él envió o transmisión de la información como reservada o confidencial de la Entidad; Sera transmitida bajo técnicas de cifrado estipuladas y aprobadas por la misma.	**Registro:** La política de controles criptográficos. Lineamiento de regulación de definición de tecnología de encriptación institucional.
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información.	3. Verificar la política de controles criptográficos.	El oficial de seguridad de la información verifica trimestral las herramientas tecnológicas, sistemas o aplicaciones que ejecuten o permitan la transmisión de la información que esta etiquetada como reservada o confidencial.	**Registro:** Formato GTE-FT-05 Informe De Estado y Gestión de controles criptográficos.
Oficial de seguridad de la información.	4. Ejecutar gestión de llaves	Se elabora un lineamiento sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo ciclo de vida.	**Registro:** Lineamiento de Gestión de llaves criptográficas
e). Seguridad física y del entorno			
Líder y/o Coordinador del	1. Diseñar la política de		**Registro:**

Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información	seguridad física y del entorno	Diseñar la política de seguridad física y el entorno donde se establece los lineamientos o guías para la utilización o administración de áreas seguras y seguridad de equipos dentro la Entidad.	La política de seguridad física y el entorno
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información	2. Realizar Verificación de áreas seguras.	Realizar la verificación de áreas seguras dentro la Entidad según la política de seguridad física y del entorno en la que se define como prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de la información. Se acoge dentro de la política las actividades de perímetro de seguridad física, controles de acceso físicos, seguridad de oficinas e instalaciones, protección contra amenazas externas y ambientales, trabajo en áreas seguras, áreas despacho y carga.	**Registro:** Formato GTE-FT-27 Lista de chequeo de áreas seguras.
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información.	3. Realizar Verificación de equipos.	Para la verificación de seguridad de los Equipos, Es necesario que el inventario de gestión de activos de tipo hardware se encuentre elaborado, actualizado y aprobado por la dirección de la Entidad. Adicionalmente, estar actualizada la matriz de inventario generada de la política de gestión de activos. Se valida el estado de los siguientes los ítems: ubicación y protección de los equipos, servicios de suministro, seguridad del cableado, mantenimiento de equipos, retiro de activos, seguridad equipos y activos fuera de las instalaciones, disposición segura o reutilización de equipos, equipo de usuario desatendido y pantalla limpia.	**Registro:** Formato GTE-FT-28 lista de chequeo de seguridad de equipos TI.
f). Seguridad de las operaciones			
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información.	1. Diseñar la política de seguridad de las operaciones.	Diseñar la política para la seguridad operativa donde se conformen los lineamientos o guías para responsabilidades y procedimientos de operación, protección contra código malicioso, copias de seguridad, registro de actividad y supervisión, control del software en explotación y gestión de la vulnerabilidad técnica cumpliendo lo establecido de acuerdo con el modelo de seguridad y privacidad de la información.	**Registro:** Política de seguridad de las operaciones.
Lider y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información. Coordinador de Talento Humano	2. Ejecutar asignación de responsabilidades operativas	La asignación de responsabilidades operativas se desarrollará de acuerdo con el rol de responsabilidades y dependiendo el área de la Entidad. Se define una guía sobre todos los recursos y servicios tecnológicos de la Entidad. Toda la documentación generada y relacionada con los servicios tecnológicos de la Entidad deber ser etiquetada y clasificada como reservada o confidencial. Debe ser guardada o almacenada donde se cumpla integridad, confidencialidad y disponibilidad.	**Registro:** Política de seguridad de las operaciones.

Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información	3. Ejecutar protección contra código maliciosos	En protección contra Códigos Maliciosos se utilizará en la Entidad el software autorizado como antivirus, antimalware, antispam y antispyware instalado y configurado en cada uno de los equipos informáticos de la plataforma tecnológica y de servicios.	**Registro:** Política de seguridad de las operaciones.
Coordinador de servicios tecnológicos. Coordinador de seguridad de la Información Coordinadores de Grupo	4. Ejecutar copias de seguridad	Las copias de respaldo de la información se elaboran y aprueban de acuerdo con la Guía de copia de respaldo y restauración de la Información. Las copias respaldo que contenga información delicada de la Entidad debe ser almacenada donde se cumpla con la integridad, confidencialidad y disponibilidad. Se verifica que el plan de backup de servicios tecnológicos cumpla con la política general de seguridad y privacidad de la información.	**Registro:** Política de seguridad de las operaciones
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información.	5. Verificar eventos de monitoreo de seguridad de la información.	Verificar eventos de monitoreo de seguridad de la información a través de equipos tecnológicos que permitan el seguimiento y trazabilidad de logs. Es necesario analizar e identificar cuáles son los recursos y sistemas que requieren un monitoreo periódico de los registros de eventos generados y almacenados dentro la Entidad.	**Registro:** Política de seguridad de las operaciones**.**
Oficial de seguridad de la información.	6. Ejecutar registro y seguimiento a la seguridad de las operaciones	Elaborar, conservar y revisar los registros de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	**Registro:** Lista de chequeo seguimiento a la seguridad de las operaciones.
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información.	7. Ejecutar control del software en desarrollo	Para el cumplimiento de control de software operacional, se identifica el tipo software operativo que está instalado en la plataforma tecnológica de la Entidad. El cual debe cumplir el modelo de seguridad y privacidad de la información y las mejores prácticas en desarrollo de software OWASP. Se establece las restricciones y limitaciones para la instalación de software operativo en los equipos que se encuentran dentro la Entidad.	**Registro:** Lista de chequeo de control del software en desarrollo
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información.	8. Ejecutar gestión de la vulnerabilidad técnica	Para poder realizar la gestión de la vulnerabilidad técnica. Se desarrolla la identificación de vulnerabilidades dentro la Entidad y se apoya mediante la aplicación de la metodología de pruebas de efectividad desarrolladas por la Entidad. Las vulnerabilidades identificadas en las pruebas efectividad recibirán un tratamiento óptimo para lograr mitigarlas según el modelo de seguridad y privacidad de la información.	**Registro:** Informe Análisis de vulnerabilidades de sistemas operativos de cliente final, servidores y de

Oficial de seguridad de la información.			aplicaciones en desarrollo. GTE-FT-05 Informe De Estado y Gestión
g). Seguridad de las comunicaciones			
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información	1. Diseñar la Política de las comunicaciones de TI.	Se establece que la Política de las comunicaciones de TI se ejecuta con la identificación de los recursos tecnológicos y servicios de la red que contiene la Entidad. Se apoya de la política de control acceso y gestión de activos que está estipulada por la Entidad para su ejecución. En la política de gestión de la seguridad de las redes se establece los lineamientos para controles de red, mecanismos asociados a los servicios de red y segregación de redes.	**Registro:** La Política de las comunicaciones de TI.
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información	2. Segregación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes y la red se deberá subdividir por grupos y dependencia para el control y seguridad de estas. Los permisos de acceso a la red estarán definidos por el perfilamiento o rol del usuario.	**Registro:** La Política de las comunicaciones de TI.
Oficial de seguridad de la información. Oficina Asesora jurídica.	3. Ejecutar la Política de las comunicaciones de TI	Para la ejecución de la Política de las comunicaciones de TI se debe definir y delimitar el alcance de la transferencia de la información. Se revisará la lista de chequeo de la trasferencia de la información. Definir los acuerdos de confidencialidad y privacidad de la información.	**Registro:** La Política de las comunicaciones de TI.
Oficial de seguridad de la información. Jefe de Oficina Asesora de Planeación e Información	4. Realizar control a redes	Se deben identificar mecanismos de seguridad, niveles de servicio y 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.	**Registro:** Formato GTE-FT-26 lista de chequeo de control a redes.
h). Relación con los proveedores			
Lider y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información.	1. Diseñar política de relacionamiento con los proveedores	Diseñar la política de relacionamiento con los proveedores; Donde se establecerá los lineamientos o guías de seguridad de la información para las relaciones laborales de la Entidad con los proveedores o terceros. De esta manera, se preserve la confidencialidad, integridad y disponibilidad de los datos institucionales. Se tendrá en cuenta para el desarrollo de la actividad: - La política de seguridad de la información para las relaciones con los proveedores.	**Registro:** La política de relación de proveedores.

Oficial de seguridad de la información. Secretaria General		- Tratamiento de la seguridad dentro de los acuerdos con los proveedores. - La cadena de suministro de productos y servicios. - Seguimiento revisión de los servicios de los proveedores. - Seguimiento a la gestión de cambios a los servicios prestados por los proveedores.	
Secretaria General. Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información.	2. Seguimiento y supervisión de los servicios de los proveedores	Se debe hacer seguimiento, revisión y auditoria mensual a la prestación de servicios de los proveedores con el objeto de medir su efectividad y cumplimiento.	**Registro:** Formato GAA-FT-11 Informe Mensual de Prestación de Servicios
Secretaria General. Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información.	3. Gestionar Cambios	Gestionar cambios en los suministros de servicios por parte de los proveedores, incluyendo el mantenimiento y mejora de las políticas procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información sistemas y procesos de negocio involucrados, y la revaluación de los riesgos.	**Registro:** Formato GTE-FT-18 de solicitud de cambios en proyectos TI.
j). Adquisición, desarrollo y mantenimiento de sistemas de información			
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información.	1. Diseñar política de seguridad en la adquisición, desarrollo y mantenimiento de sistemas de información.	Diseñar la política de seguridad en adquisición, desarrollo y mantenimiento de sistemas de información, donde se establecerá los lineamientos que garanticen que los sistemas de información desarrollados o adquiridos por la Entidad.	**Registro:** La política de seguridad en la adquisición, desarrollo y mantenimiento de sistemas de información.
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información.	2. Analizar y especificar requisitos de seguridad de los sistemas	Velar por que se cumpla con los requisitos de seguridad de la información en la adquisición, desarrollo y mantenimiento de los sistemas de información o para mejorar de sistemas existentes. Que la seguridad de la información sea una parte integral durante todo el ciclo de vida.	**Registro:** Informe de requisitos de seguridad de los sistemas de información.

Oficial de seguridad de la información.	de información.	Para el cumplimiento de los requisitos de seguridad de los sistemas de información se tendrán encuentra los siguientes ítems: - Análisis y especificación de requisitos de seguridad de la información - Seguridad de servicios de las aplicaciones en redes públicas. - Protección de transacciones de los servicios de las aplicaciones. Se deberá cumplir con la política de seguridad en las operaciones, en lo que respecta a la utilización de las mejores prácticas de desarrollo de software (OWAS)	Formato GTE-FT-05 Informe de Estado y Gestión
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información.	3. Ejecutar seguridad en los procesos de desarrollo y soporte.	Se utiliza una metodología ágil para el desarrollo (QA) de software que permita contemplar como mínimo: control de cambios en sistemas, revisión técnica de las aplicaciones después de cambios en la plataforma de operación, restricciones en los cambios a los paquetes de software, principio de construcción de los sistemas seguros, ambiente de desarrollo seguro, desarrollo contratado externamente, pruebas de seguridad de sistemas, prueba de aceptación de sistemas y protección de la transacciones de los servicios de las aplicaciones.	**Registro:** La política de seguridad en la adquisición, desarrollo y mantenimiento de sistemas de información.
Líder de desarrollo y mantenimiento. Oficial de seguridad de la información.	4. Ejecutar datos de prueba.	La ejecución de datos de prueba se asegura la protección de datos usado para pruebas. Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	**Registro:** Formato GTE-FT-20 Plan de pruebas de software.
k). Gestión de incidentes de seguridad de la información			
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información.	1. Diseñar la política de gestión de incidentes de seguridad de la información.	Diseñar la política de gestión de incidentes de seguridad de la información donde se establecerán los lineamientos o guías que asegurara una gestión de incidentes seguridad y óptima. Incluida, la comunicación sobre eventos de seguridad y debilidades que afecten la preservación de la confidencialidad, integridad y disponibilidad de la información de la Entidad.	**Registro:** La política de gestión de incidentes de seguridad de la información.
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información.	2. Definir responsabilidades y actividades.	Establecer responsabilidades y actividades de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	**Registro:** La política de gestión de incidentes de seguridad de la información.
Oficial de seguridad de la información.	3. Realizar reporte de eventos de	Los eventos de seguridad de la información se deberán informar a través del centro de servicios tan pronto como sea posible.	**Registro:** Informe de gestión de

	seguridad de la información	Se debe elaborar un informe bimensual de gestión de incidentes de seguridad de la información.	incidentes de seguridad de la información GTE-FT-05 Informe De Estado y Gestión
Oficial de seguridad de la información.	4. Realizar reporte de debilidades de seguridad de la información	Se debe exigir a todos los funcionarios contratistas y terceros que usan los servicios y sistemas de información de la Entidad, a que reporten por el centro de servicios cualquier debilidad de seguridad de la información observada o sospechosa en los mismos.	**Registro:** Informe de gestión de incidentes de seguridad de la información Formato GTE-FT-05 Informe De Estado y Gestión.
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información.	5. Realizar evaluación de los eventos de seguridad de la información y toma de decisiones	Evaluar todos los eventos de seguridad y estos se deberán clasificar como incidentes o eventos de seguridad, para dar respuesta al incidente de forma adecuada.	**Registro:** Informe de gestión de incidentes de seguridad de la información Formato GTE-FT-05 Informe De Estado y Gestión
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información.	6. Dar respuesta a incidentes de seguridad de la información.	Se da repuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados y estandarizados al respecto y teniendo en cuenta el FAQS tabla de preguntas y repuestas frecuentes.	**Registro:** Herramienta Centro de servicios. Informe de gestión de incidentes de seguridad de la información Formato GTE-FT-05 Informe De Estado y Gestión.
Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información	7. Registrar el aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se deberá usar para reducir la posibilidad o impacto de incidentes futuros. También se tendrá que registrar en la tabla de FAQS de gestión de incidentes de seguridad.	**Registro:** Novedades de FAQ'S
Líder y/o Coordinador del Grupo de Gestión de las	8. Hacer recolección de evidencia digital.	La Entidad deberá definir y aplicar procedimientos para la identificación recolección adquisición y preservación de la información, que pueda servir como evidencia.	**Registro:** Lineamiento de cadena de custodia de

Tecnologías de la Información. Oficial de seguridad de la información		Se deberá establecer lineamiento de cadena de custodia de evidencia digital.	evidencia digital.
l). Seguridad de información de la gestión de continuidad de negocio			
Líder de Infraestructura. Líder y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Oficial de seguridad de la información. Jefe de Oficina Asesora de Planeación e Información	1. Planear la continuidad de la seguridad de la información	Se determinan los requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas contemplando crisis o desastres.	**Registro:** Matriz de riesgos.
Lider y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información. Jefe de Oficina Asesora de Planeación e Información. Oficial de seguridad de la información. Secretaria General.	2. Implementar la continuidad de la seguridad de la información	Establecer, documentar, implementar y mantener procesos, procedimientos y control para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación de riesgo.	**Registro:** La política de seguridad de la información de la gestión del negocio.
Control de Interno. Oficial de seguridad de la información. Lider y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información.	3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Verificar de forma trimestral los controles de continuidad de la seguridad de la información establecidos e implementados con el fin de asegurar de que son válidos y eficaces durante situaciones de riesgo.	**Registro:** Lista de chequeo de efectividad de controles de gestión de continuidad de seguridad de la información
Lider y/o Coordinador del Grupo de Gestión de las Tecnologías de la Información.	4. Asegurar la disponibilidad de instalaciones de procesamient	Las instalaciones de procesamiento de la información (Centro de datos) se deben implementar con redundancia suficiente para cumplir con los requisitos de continuidad.	**Registro:** Informe de condiciones de seguridad de instalaciones de

	o de información.		procesamiento de la información. Formato GTE-FT-05 Informe De Estado y Gestión.

CONTROL DE CAMBIOS			
VERSIÓN INICIAL	**DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO**	**FECHA**	**VERSIÓN FINAL**
00	• Se crea procedimiento de acuerdo a las necesidades del Grupo de Gestión de las Tecnologías de la Información.	29/08/2018	**01**