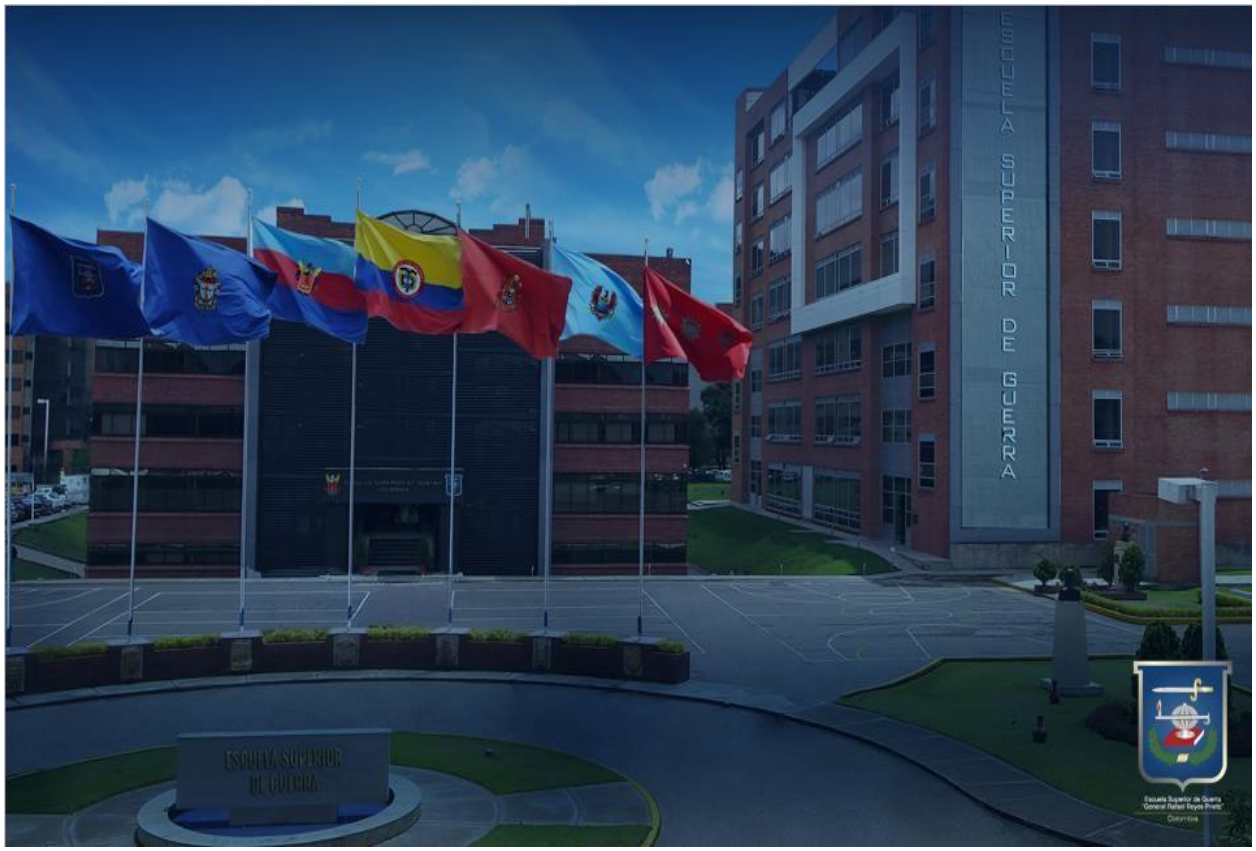
# MANUAL DE POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION




**DEPARTAMENTO TIC**

**ESCUELA SUPERIOR DE GUERRA “GENERAL RAFAEL REYES PRIETO”**

**Bogotá, D.C., 2023**

## TABLA DE CONTENIDO

**INTRODUCCION**

Para la Escuela Superior de Guerra “General Rafael reyes Prieto”, en adelante la ESDEG, la información es un activo de alta importancia para la entidad, por consiguiente, es necesario implementar reglas y medidas que permitan proteger la disponibilidad, integridad y confidencialidad en todo el ciclo de vida de la información.

El presente documento está orientado a proteger los activos de información en los ambientes relacionados con TIC, en los cuales se procesan, operan, almacenan, transmiten o usan y estén sometidos a los controles correspondientes para su adecuada protección; a garantizar el uso apropiado de los dispositivos tecnológicos (computadores de escritorio, portátiles, etc.) y de servicios como Internet y el correo electrónico; a brindar a los usuarios pautas para la utilización apropiada ; y a contribuir a minimizar los riesgos de una eventual pérdida de los activos de información de la ESDEG.

Se establecen las Políticas Generales en Seguridad de la Información, alineados con la norma ISO 27001 de 2013 (buenas prácticas en seguridad de la información) y siguiendo el Modelo de Seguridad y Privacidad de la Información (MSPI), las cuales ayudarán a ofrecer servicios seguros, confiables y oportunos en la Entidad, como lo dictan las directrices de Gobierno Digital, para brindar mayor confianza de los ciudadanos hacia las instituciones del estado.

El Manual y políticas de Seguridad de la Información, da las directrices que deben cumplir los alumnos, docentes, personal de planta, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la ESDEG, con el fin de asegurar un adecuado nivel de confidencialidad, integridad y disponibilidad en su información.

La ESDEG, a través del Comité Institucional de Gestión y Desempeño, estudiará y aprobará todas las iniciativas, acciones que sean necesarias para la implementación del SGSI y velará por el cumplimiento de las políticas establecidas en el presente manual.

## 1. OBJETIVO

Establecer lineamientos relacionados con la seguridad de la información abordando temáticas específicas, como complemento a lo definido en la “Política General de Seguridad de la Información de la ESDEG” con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de la ESDEG.

## 2. ALCANCE

Las políticas contenidas en el presente manual aplican a todos los alumnos, docentes, personal de planta, contratistas, visitantes y terceros de la ESDEG que por alguna razón tengan cualquier tipo de interacción con los activos de información

## 3. APLICABILIDAD DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACION

Las políticas contenidas en el presente manual aplican y son de obligatorio cumplimiento para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información.

## 4. REFERNCIAS NORMATIVAS

- Ley 1581 del 17 de octubre de 2012. “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- Ley 1712 del 06 de marzo 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 1078 de 2015 del 26 de mayo de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- Decreto 612 del 4 de abril 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”

- Decreto No. 1008 del 14 de junio 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" A partir de este Decreto se cambia el modelo anterior de la Estrategia de Gobierno en Línea, para dar paso a la Política de Gobierno Digital.
- Decreto 620 del 02 de mayo de 2020 “Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 Y 64 de la Ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales”.
- Decreto 088 del 24 de febrero de 2022 “Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3o, 5o y 6o de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea”
- Decreto 767 del 16 de mayo de 2022 “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".
- Resolución No. 09 del 20 de abril de 2018. Por el cual se creó y conformo los Comités Institucional y Operativo de Gestión y Desempeño.
- Resolución 01519 del 24 de agosto de 2020 “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”
- Resolución 2160 del 23 de octubre de 2020 “Guía de servicios ciudadanos digitales y guía para vinculación de uso de estos”.
- Resolución 02893 del 30 de diciembre de 2020 “Por la cual se expiden los lineamientos para estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPAs y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado Colombiano, y se dictan otras disposiciones”
- Resolución 500 de 10 de 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”.
- Resolución Número 000460 de 15 de febrero 2022 “Por la cual se expide el Plan Nacional de Infraestructura de datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación”.
- Resolución 01117 de 5 de abril de 2022. “Por la cual se establecen los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el marco de la Política de Gobierno Digital”
- Directiva permanente Ministerio de Defensa No. 018 de 2014. Políticas de seguridad de la información para el Sector Defensa.
- Directiva Permanente No. 03 del 23 de enero de 2019. “Lineamientos para la definición de la Política de Tratamiento de Datos personales en el Ministerio de Defensa Nacional”.
- Directiva Presidencial 02 del 24 de febrero de 2020 “Reiteración de la Política en materia de Seguridad Digital. Presidencia de la República”.
- Directiva Presidencial 03 de 15 de marzo de 2021 “Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos”.
- Directiva Presidencial No. 02 de 24 de febrero de 2022. “Reiteración de la Política en materia de Seguridad Digital”.
- Norma técnica colombiana NTC-ISO-IEC 27001:2013. Norma Técnica de sistemas de gestión y se dictan otras disposiciones.
- Documento CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- Documento CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- Documento CONPES 3920 DE 2018. Política Nacional para la Explotación de Datos (Big Data).
- Documento Conpes 3975 de 08 de noviembre e 2019 “Política Nacional para la Transformación Digital e Inteligencia Artificial”.
- Documento Conpes 3995 de 01 de junio de20220 “Política Nacional de Confianza y Seguridad Digital.

- Acta No. 1435 del 08 de octubre de 2018 de Reunión de Comité Institucional de gestión y desempeño.
- Acta No. 640 del 10 de abril de 2019 de Reunión de Comité Institucional de gestión y desempeño.
- Acta No. 0782 del 08 de abril de 2021 de Reunión de Comité Institucional de gestión y desempeño

## 5. TERMINOS Y DEFINICIONES

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

**Amenaza:** Según [ISO IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

**Análisis de riesgos:** A partir del riesgo definido, se define las causas del uso sistemático de la información para identificar fuentes y estimar el riesgo.

**Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

**Autenticidad:** Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.

**Confiabilidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.

**Controles:** Medida que permite reducir o mitigar un riesgo.

**Desastre**: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

**Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.

**Evento:** Según [ISO/IEC 27000): Ocurrencia o cambio de un conjunto particular de circunstancias. Un evento de seguridad es cualquier ocurrencia observable que sea relevante para la seguridad de la información. Esto puede incluir intentos de ataques o fallos que descubren vulnerabilidades de seguridad existentes.

**Evidencia objetiva:** Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

**Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

**Impacto:** Resultado de un incidente de seguridad de la información.

**Incidente:** Según [ISO IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometerlas operaciones del negocio y amenazar la seguridad de la información.

**Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento quelos sujetos obligados generen, obtengan, adquieran, transformen o controlen. Constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

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

**Ingeniería Social:** Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red o faciliten información con clasificación confidencial o superior. En el campo de la seguridad informática, es un método o forma de ataque con técnicas que buscan persuadir al atacado ganando su confianza, obteniendo información privilegiada de carácter personal (contraseñas de cuentas bancarias, datos personales), igualmente apropiarse de información vital para una organización. Existen en la actualidad diversidad de medios para llevar acabo esta actividad, un uso común es a través de correos electrónicos o llamadas al lugar de trabajoo residencia, de ahí la importancia de tener una buena cultura digital respecto a que información suministramos.

**Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.

**Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
**Parte interesada:** Según Norma ISO/IEC 27000, Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad.
**Plan de continuidad del negocio (Bussines Continuity Plan):** Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.
**Política de seguridad:** Definición en la cual se establece el compromiso de la Dirección y el enfoquede la organización en la gestión de la seguridad de la información.
**Propiedad intelectual**: es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.
**Propietario de la información**: es la unidad organizacional o proceso donde se crean los activos de información.
**Proceso:** Según la norma ISO/IEC 27000, Conjunto de actividades interrelacionadas o interactivas que transforman entradas en salidas.
**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 y la optimización del trabajo al interior de la ESDEG.
**Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
**Seguridad de la información:** Según [ISO IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.
**Sistema de Gestión de la Seguridad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
**Sensibilización**: es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.
**Sistema de información**: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la ESDEG o de origen externo ya sea adquirido por la Entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.
**Sniffers:** Programa de captura de las tramas de red. Generalmente se usa para gestionar la red conuna finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.
**Software malicioso**: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.
**Teletrabajo**: Hace referencia a todas las formas de trabajo por fuera de la oficina, incluidos los entornos de trabajo no tradicionales, a los que se denomina "trabajo a distancia", "lugar de trabajo flexible", "trabajo remoto" y ambientes de "trabajo virtual".
**Troyano:** Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadaspara sobrepasar los sistemas de seguridad.
**Usuario:** en el presente documento se emplea para referirse a directivos, funcionarios, contratistas,terceros y otros colaboradores de la ESDEG, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la ESDEG y a quienes se les otorga un nombre de usuario y una clave de acceso.
**Virus:** Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamientode una red de sistemas o computador personal, por lo general su acción es transparente al usuarioy este tardo tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

**VPN** (Virtual Private Network- Red privada virtual): es una tecnología de red que permite una extensión segura de la redprivada de área local (LAN) sobre una red pública o no controlada como Internet.
**Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO IEC 13335-1:2004]:debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

## 6. ABREVIATURAS, UNIDADES DE MEDIDA Y EXPRESIONES ACEPTADAS

DETIC: Departamento TIC.
ESDEG: Escuela Superior de Guerra “General Rafael Reyes Prieto”
FTP: Protocolo de Transferencia de Archivos
ISO: Norma Técnica Internacional.
MINTIC: Ministerio de las Tecnologías de la Información y Comunicaciones.
TCP: Protocolo de Control de Transmisión.
TIC: Tecnologías de la información y la Comunicación.
TI: Tecnologías de la información.
SGSI: Sistema de Gestión de Seguridad de la información.

## 7. POLITICAS

LA ESDEG a través de DETIC, establece a continuación, los siguientes lineamientos de seguridad de la información, los cuales deberán ser cumplidos por todos los alumnos, funcionarios, contratistas, terceros, usuarios y visitantes. Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la entidad.

A continuación, se determinan las Directrices seguir:

### 7.1 POLITICAS DE SEGURIDAD DE LA INFORMACION

Se debe verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.

Se debe establecer un programa que permita el fomento continuo de la creación de cultura y conciencia de seguridad en los alumnos, funcionarios, contratistas, proveedores, personas, usuarios de los sistemas de información y telecomunicaciones de la ESDEG.

Todos los usuarios de los sistemas de información y telecomunicaciones de la ESDEG tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en el presente Manual de Políticas de Seguridad de la Información.

Con la gestión de riesgos de seguridad de la información, se busca mediante la aplicación de las diferentes etapas preservar la confidencialidad, integridad y disponibilidad de la información, por lo tanto, con los controles y la evaluación de su aplicación en el monitoreo se avalúa la eficacia de su aplicación.

Diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la información - SGSI, los cuales estarán a cargo de la Oficina de Planeación Estratégica que hace las veces de la Oficina de Control Interno.

La ESDEG debe contar con dispositivos y sistemas de seguridad perimetral para la conexión a Internet o cuando sea inevitable para la conexión a otras redes en outsourcing o de terceros.

Los jefes de Área o dependencia deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realicen correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de la ESDEG.

LA ESDEG aplica los Controles del Anexo A de la Norma NTC: ISO/IEC 27001:2013 y dominios a los que pertenece.

## 7.2 POLIITCA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

La ESDEG genera un esquema de seguridad de la información creando un Comité de seguridad de la información y definiendo la asignando roles y responsabilidades que involucran actividades de gestión, administración y operación de la seguridad de la información.

La actualización y reorganización del organigrama y las funciones y responsabilidades ya sea por cargos y/o responsabilidades se hará en concordancia con el sistema de gestión integrado.

### 7.2.1 Política de Organización Interna

7.2.1.1 Asignación de roles y responsabilidades

La ESDEG Mediante Acta No. 0782 del 08 de abril de 2021 en Reunión de Comité Institucional de Gestión y Desempeño, aprobó los Roles y Responsabilidades de Seguridad de la Información en el Numeral 10. Políticas Institucionales de Gestión para TIC.

7.2.1.2 Separación de deberes

- Cada funcionario tendrá funciones y áreas de responsabilidad separadas, para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de activos informáticos de la ESDEG.
- Se establecerán controles que permitan realizar auditorías, supervisión de las actividades por los técnicos responsables de la infraestructura de red de la y sistemas de información.

**7.2.1.3** Política contacto con las autoridades

- La ESDEG establecerá procedimientos que especifiquen cuándo y a través de que autoridades se deben contactar y la forma en que se deben reportar oportunamente los incidentes identificados de la seguridad de la información, si se sospecha de incumplimiento de la ley.
- El mantenimiento de dichos contactos debe ser un requisito para dar soporte a la gestión de incidentes de seguridad de la información o la continuidad de la Institución y el proceso de planes de contingencia.
- Los contactos con otras autoridades incluyen servicios públicos, servicios de emergencia, salud y seguridad, como el departamento de bomberos (en conexión con la continuidad de la Institución), proveedores de telecomunicaciones con enrutamiento en línea, disponibilidad) y proveedores de agua con medios de refrigeración para los equipos).

7.2.1.4 Política contactos con grupos de interés especial

Los funcionarios pertenecientes al comité de Seguridad y Privacidad de la Información se deben contactar entre sí y pertenecer a foros o grupos de interés especial en Seguridad de la Información y manejo de evidencia digital para:

- Mejorar el conocimiento sobre las mejores prácticas y estar actualizado con la información pertinente a la seguridad.
- Garantizar que la comprensión del entorno de seguridad de la información sea actual y completa.
- Recibir advertencias oportunas de alertas, avisos y parches relacionados con ataques y vulnerabilidades.
- Obtener acceso a asesoría especializada sobre seguridad de la información.

- Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.
- Suministrar puntos adecuados de enlace cuando se trata de incidentes de seguridad de la información.
- Se pueden establecer acuerdos para compartir información con el objeto de mejorar la cooperación y la coordinación de los temas de seguridad con organismos afines externos. Dichos acuerdos deben identificar los requisitos para la protección de la información sensible o clasificada.

7.2.1.5 Política de seguridad de la información en la gestión de proyectos

La seguridad de la información en la gestión de proyectos debe ser incorporada desde la conceptualización de la solución, entendiendo en la fuente con las expectativas de la ESDEG, el nivel de sensibilidad de la información, los impactos que se tiene en las metas estratégicas y las responsabilidades que dicha información genera para la entidad.

Los funcionarios deberán estar notificados, de al menos, algunas prácticas que se llevan a cabo para concretar soluciones de negocio, que cumplan con las especificaciones requeridas de funcionalidad y el marco de seguridad y control base, que aseguren el debido cuidado de la entidad frente al reto de la inevitabilidad de la falla en el desarrollo, entrega y puesta en operación de una solución de software o tecnología de información:

- Identificar los activos digitales y de información claves que estarán involucrados en el desarrollo de la solución
- Determinar las responsabilidades legales que tiene la entidad con la información que se modela y fluye en la solución de negocio (incluidos los grupos de interés afectados).
- Establecer el nivel de sensibilidad de la información que la aplicación utilizará y las medidas de seguridad y control requeridas para asegurarla de acuerdo con dicho nivel.
- Consultar los informes de auditoría previos que afectan el proceso que se interviene con el proyecto de implementación de software, con el fin de atender y asegurar los hallazgos que sean pertinentes para su alcance.
- Configurar el estándar de debido cuidado necesario y suficiente para atender los retos propios del desarrollo de aplicaciones, que atienda las exigencias de los entes de control, el perfil de riesgo del negocio y las expectativas de la gerencia frente a sus objetivos estratégicos.

### 7.2.2 Política dispositivos móviles y teletrabajo

7.2.2.1 Política para dispositivos móviles

- La ESDEG establece las condiciones para el uso seguro de los dispositivos móviles (portátiles, teléfonos inteligentes, tabletas, entre otros) institucionales que hagan uso de servicios de la Entidad como son: Establecer contraseñas de acceso robustas, cifrar la información almacenada, mantener el dispositivo móvil con el sistema operativo siempre actualizado y con un antivirus activo.
- Los funcionarios y contratistas no están autorizados a cambiar la configuración ni la instalación/desinstalación de las aplicaciones móviles de los dispositivos institucionales que se les entregue como recurso para la ejecución de sus obligaciones o funciones.
- Es responsabilidad del servidor público al que se le asigno el dispositivo móvil evitar la instalación de programas desde fuentes desconocidas, evitar el uso de redes inalámbricas públicas y mantener desactivadas las redes inalámbricas como WIFI, Bluetooth o infrarrojos en los dispositivos móviles institucionales asignados.
- Los funcionarios y contratistas deben evitar conectar los dispositivos móviles institucionales a puertos USB de computadores públicos, hoteles o cafés internet, terminales y demás sitios de acceso público.
- Cuando se tratan temas laborales mediante dispositivos móviles, los que intervienen en la conversación deben tener precaución de no ser víctimas de escuchas intrusivas.

- Los servidores públicos y contratistas deben notificar los dispositivos móviles institucionales con sospecha de infección por malware al personal técnico responsable de DETIC para el proceso de análisis, evaluación y tratamiento.
- Los dispositivos móviles que son autorizados para salir de las instalaciones por parte de la ESDEG deben ser protegidos mediante el uso e implementación de los controles apropiados como cifrado de información, políticas de restricción en la ejecución de aplicaciones y de conexión de dispositivos USB, inactivación de accesos inalámbricos cuando se encuentren conectados a la red LAN de la ESDEG, entre otros.
- Todos los dispositivos móviles propiedad de la ESDEG pueden ser monitoreados y sometidos a la aplicación de controles en cuanto tipo, versión de aplicaciones instaladas, contenido restringido y de ser necesario se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos.

7.2.2.2 Política para teletrabajo

- El DETIC establece el proceso de implementación de teletrabajo de acuerdo con la normativa y los lineamientos exigidos con el fin de proteger la información.
- La ESDEG brinda los lineamientos de seguridad digital para la protección de la información a la que se tiene acceso, se procesa o almacena en lugares en los que se realiza teletrabajo y se hace uso de los recursos tecnológicos autorizados por la ESDEG para el desarrollo de las actividades de teletrabajo.
- Toda información gestionada por la ESDEG, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales con esta.
- DETIC debe establecer los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos o partes interesadas, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.
- El DETIC revisa la seguridad física y del entorno del sitio donde se va a teletrabajar con el fin de proteger la confidencialidad, integridad y disponibilidad de la información.

## 7.3 POLITICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS

Durante el proceso de selección de personal de planta o contratistas, se realizará verificación de antecedentes disciplinarios de los candidatos sin importar el cargo o posición al cual se postulen.

Todo el personal que labore en la entidad o preste servicios a la misma deberá firmar un acuerdo de confidencialidad y un documento de conocimiento y aceptación de las políticas definidas para el sistema de seguridad de la información y buen uso de los activos de información. Mediante el cual se compromete a realizar un adecuado uso de estos.

### 7.3.1 Política antes de asumir el empleo

- El Departamento de Talento Humano o las demás encargadas de contratación de personal o por asignación de nuevos cargos con responsabilidades sobre información y activos informáticos, deberán poner especial atención en la etapa pre-laboral, para que los aspirantes cumplan con los requisitos de idoneidad y requisitos de seguridad mínimos establecidos en las políticas de Seguridad de la Información con el fin de reducir el riesgo de robo, fraude o uso inadecuado de los activos informáticos y las instalaciones.
- Se deben proteger en las áreas –físicas y lógicas- todos los activos contra acceso, divulgación, modificación, destrucción o interferencia no autorizados. Tanto los asignados para su cumplimiento, como los que se encuentren en el área de su alcance.
- Todos el personal (alumnos, personal de planta, docentes, contratistas y demás partes interesadas) que tengan acceso a información sensible deberá firmar un acuerdo de confidencialidad y un documento de

conocimiento y aceptación de las políticas definidas para el sistema de seguridad de la información y buen uso de los activos de información. Mediante el cual se compromete a realizar un adecuado uso de estos.

- Se deberá informar al funcionario, el contratista o usuario de tercera parte sobre las acciones de carácter legal, administrativo, penal, disciplinario o civil, a que puede estar sujeto si viola u omite el cumplimiento de las normas de seguridad establecidas en la institución.
- Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con la ley, reglamentos y ética pertinentes y deben ser proporcionales a los requisitos del cargo, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
- Todo el personal debe ser debidamente informados sobre sus roles y responsabilidades, así como de los acuerdos de confidencialidad y política de seguridad y privacidad de la información.
- El personal con responsabilidades y roles privilegiados debe identificarse y ser objeto de sensibilización y capacitación en aspectos de seguridad y privacidad de la información.
- En la elaboración de los contratos se deben incluir las responsabilidades del contratista y las de la organización en cuanto a la seguridad y privacidad de la información, antes durante y después del cumplimiento del contrato.

### 7.3.2 Política durante la ejecución del empleo

- Informar al funcionario, contratista o usuario de tercera parte, sobre las funciones y las responsabilidades respecto a la seguridad de la información antes de que se le otorgue acceso a la información o a los sistemas de información sensibles o clasificados.
- Cumplir las políticas de seguridad y privacidad de la información.
- Desarrollar los procesos de concientizar y sensibilizar al personal, sobre la Seguridad de la Información, sus funciones y responsabilidades dentro de la Institución.
- Verificar permanentemente el cumplimiento de las políticas de seguridad por parte de todo el personal y ordenar los estudios de seguridad que considere pertinentes; así como la actualización de la matriz de riesgos. Aplicar y actualizar la documentación requerida al personal (promesas de reserva y formatos de autorización de servicios informáticos, estudios de seguridad de personal, tarjetas de manejo de documentación, promesa de reserva, contratos de prestación de servicios, etc.) de acuerdo con la normatividad vigente.
- Los procedimientos disciplinarios para emprender acciones contra empleados públicos o contratistas que cumplen funciones públicas, que hayan cometido una violación a la seguridad de la información se harán de acuerdo con la ley.

### 7.3.3 Política terminación y cambio de empleo

- Proteger los intereses de la Entidad como parte del proceso de cambio o terminación de empleo.
- Se deberá formalizar el proceso de terminación de la relación laboral, para incluir la devolución del software previamente desarrollado dentro de la Institución, los documentos corporativos y los activos informáticos asignados.
- El departamento de Talento Humano o la dependencia encargada del control del personal que termina su relación laboral, contrato o convenio, o que es reasignada a una nueva función o cargo, deberá informar de manera inmediata la novedad presentada al DETIC y/o al Oficial de Seguridad de la Información con el fin de que tomen las acciones inmediatas para cancelar o revocar los permisos o autorizaciones de acceso y la devolución y restitución de activos informáticos.
- Los derechos de acceso que se deben adaptar o retirar incluyen acceso físico y lógico, claves, tarjetas de identificación, servicios de procesamiento de información, suscripciones y retiro de cualquier documentación que lo identifique como miembro actual de la organización.
- Cuando un funcionario, contratista o usuario de terceras partes con autorización especial con términos de uso definidos, usa uno o más equipos de la organización o utiliza su propio equipo, se debe aplicar un procedimiento especial de seguridad, durante el tiempo de su uso y al término, garantizar que toda la información pertinente se transfiere a la ESDEG y se elimina con seguridad de tales activos informáticos.

- Cuando un funcionario, contratista o usuario de terceras partes tiene un conocimiento especial que es importante para la continuación de las operaciones informáticas, esa información o conocimiento, debe estar documentada y transferirse a la organización.

## 7.4 POLITICAS DE GESTION DE ACTIVOS

Toda información sea física o digital generada, almacenada o transformada por los funcionarios, contratistas o proveedores de la entidad, utilizando los recursos dispuestos por la entidad para tal fin o en desempeño de sus labores o servicio contratado, son activos de información **propiedad de la ESDEG.**

Los activos dispuestos por la ESDEG para el apoyo de las labores desempeñada por los funcionarios, contratistas o proveedores, únicamente se permitirá su utilización para ejecución de tareas establecidas en el ámbito laboral de la ESDEG.

La ESDEG identificará, clasificará y gestionará su inventario de activos conforme a los manuales y procedimientos de Gestión de Activos formalizados.

### 7.4.1 Política de responsabilidades de los activos

7.4.1.1 Política Inventario de activos

- La ESDEG identificará, clasificará y gestionará su inventario de activos conforme al procedimiento de identificación y clasificación de activos de información y el formato de inventario y clasificación activos de información formalizados. Así mismo se debe asignar un responsable para su conservación y control.
- Es responsabilidad del líder del proceso, jefe de área o directo, la identificación y reporte de nuevos activos de información, así mismo mantener actualizada la valoración de estos.

7.4.1.2 Política propiedad de los activos

- Cada activo mantenido en los inventarios debe tener un propietario.
- Todos los activos de información deben contar con un responsable que asegure la protección de la información y los datos que son almacenados en cada uno de ellos.

7.4.1.3 Política uso aceptable de los activos.

- El uso aceptable de los activos de información implica la aceptación implícita por parte de los usuarios de estos, de las normas, políticas y estándares establecidos para garantizar la Seguridad de la Información y el buen uso de los mismos, así como de los compromisos y responsabilidades adquiridas.
-
- Las dependencias y funcionarios de la ESDEG podrán usar, monitorear y supervisar la información, sistemas, servicios, equipos e instalaciones que le sean asignados para el cumplimiento de sus funciones, de acuerdo con la establecido en esta política, las funciones propias, los manuales de uso y la legislación vigente.
-
- El personal debe evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de la información almacenada en los medios.

7.4.1.4 Política devolución de Activos

- Al momento de la desvinculación o de cambio de roles, todo funcionario y/o tercero debe hacer entrega de todos los activos de información que le hayan sido asignados. Estos mediante el formato establecido por la entidad.
- Empleados y usuarios externos deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

### 7.4.2 Política de clasificación de la Información

7.4.2.1 Política clasificación de la información

- Toda la información deberá ser identificada, clasificada y documentada con base en los criterios de clasificación definidos en Guía para la Gestión y Clasificación de Activos de Información de MinTIC y la directiva de clasificación de documentación reservada de las Fuerzas Militares.
-
- Los propietarios de los activos de información son los responsables de establecer el nivel de clasificación de cada activo.

7.4.2.2 Política etiquetado de la información

- Todos los activos de información de la ESDEG, cuales fuere su medio de almacenamiento deben ser objeto de un control sobre su gestión para administrar su contabilidad e inventario.
- En el caso de los equipos informáticos, cada parte de equipo le será asignado un número de inventario que se ate al número de serie, MAC (Media Access Control address) y modelo del equipo o parte. Las etiquetas se colocarán estratégicamente en sitio visible de cada parte conteniendo el número de inventario y su identificación, así como el propietario del recurso.
- Los documentos deben ser etiquetados de acuerdo con la normatividad vigente de gestión documental.

7.4.2.3 Política manejo de activos

- Para el plan de evacuación se deben marcar de manera especial los activos informáticos que contengan información de inteligencia, operaciones, proyectos y planes especiales de las Fuerzas Militares, o información sensible o clasificada.
- El Oficial de Seguridad de la Información es el responsable de establecer y determinar qué equipos de comunicaciones, servidores y equipos de cómputo deben ser evacuados en orden de prioridades en caso de evacuación.
- Así mismo, los equipos que por su arquitectura, información, tecnología, capacidades o importancia, pudieran comprometer la Seguridad y Defensa Nacional, si cayeran en posesión del enemigo o terceros con el fin de priorizar y determinar el proceso de destrucción de los mismos en caso de abandono de la unidad. Esto debe ser realizado mediante una etiqueta especial fijada en una parte visible.

### 7.4.3 Política de manejo de medios

7.4.3.1 Política gestión de medios removibles

- Los medios de almacenamiento removibles como cintas, discos duros, CDs, DVDs, dispositivos USB, entre otros, así como los medios impresos que contengan información institucional, debe ser controlados y físicamente protegidos.
- El DETIC definirá los medios removibles de almacenamiento que podrán ser utilizados por las personas autorizadas en los sistemas de información y en la plataforma tecnológica en caso de ser requerido para el cumplimiento de sus funciones.
- Cada medio removible de almacenamiento deberá estar identificado de acuerdo con el tipo de información que almacene, dando cumplimiento a los lineamientos establecidos en el procedimiento de inventario y clasificación de activos de información, si un medio removible llegase a contener información con distintos niveles de clasificación, será clasificado con la categoría que posea el mayor nivel de clasificación.

7.4.3.2 Política disposición de los medios

- Para los procesos de baja, de reutilización o de garantía de los dispositivos que tengan medios de almacenamiento, se debe cumplir según sea el caso con la destrucción física del mismo o borrado seguro. la destrucción segura se documentará mediante acta, registro fílmico y fotográfico.

7.4.3.3 Política transferencia de medios Físicos

- El tránsito o préstamo de medios removibles deberá ser autorizado por el propietario de dicho activo.
- Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

## 7.5 POLITICAS DE CONTROL DE ACCESO

Para la protección de los activos de información, se establecerán procedimientos y políticas para el control de acceso a la red, sistemas de información e infraestructura física (Instalaciones). Con el fin de mitigar los riesgos asociados al acceso no autorizado a la información.

Todos los usuarios deberán asumir la responsabilidad sobre la información física o digital que accedan y procesan dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información

### 7.5.1 Política requisitos de la ESDEG para el control de acceso

7.5.1.1 Política de Control de acceso

Para acceder a los servicios tecnológicos la persona debe tener relación laboral con la ESDEG.

El acceso a la red de la Entidad debe ser otorgado solo a usuarios/as autorizados/as, previa definición, verificación y control de los perfiles y roles, otorgados por el/a jefe/a inmediata en coordinación con el Departamento de Talento Humano, cuya implementación es responsabilidad de DETIC.

Todos los funcionarios y partes interesadas deben seguir los procedimientos y formatos establecidos por DETIC en lo relacionado a la asignación de usuarios y contraseñas, para poder acceder a los servicios de red de la Entidad, a los recursos de la plataforma tecnológica o a los sistemas de información.

DETIC establece los mecanismos necesarios para realizar conexiones seguras a los servicios de red y a la información, desde cualquier lugar y/u origen, lo cual incluye accesos remotos y teletrabajo para los funcionarios que por su labor así lo requieran.

La información generada o almacenada en medios institucionales es de propiedad de la ESDEG y debe ser utilizada exclusivamente para las tareas propias de las funciones desarrolladas en la entidad.

7.5.1.2 Política acceso a redes y a servicios en red

Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente

Todos los usuarios con acceso a un sistema de información o a la red informática de la ESDEG dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña, serán responsables de las acciones realizadas por el usuario que les ha sido asignado.

Todo equipo conectado a la red LAN de la ESDEG tendrá acceso a través de la dirección IP definida.

Conexiones Remotas

- La conexión remota a la red de área local de la ESDEG debe realizarse a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y monitoreada por DETIC.
- Al usar la tecnológica VPN - Virtual Private Network (Red privada virtual), se busca prevenir la interceptación de posibles atacantes en la conexión (este tipo de ataques son denominados “hombre en el medio”). Este tipo de conexión es segura por la aplicación de una capa de cifrado y autenticación en la ruta de la comunicación (denominado túnel de comunicación).
- Toda sesión de teletrabajo requerida por un usuario debe ser previamente autorizado mediante el Formato de solicitud de usuarios VPN el cual debe ser entregado en el DETIC.
- Una vez el DETIC, realiza el requerimiento ya sea a través de una VPN (Red Privad Virtual) o cualquier solución definida que debe proveer conexión segura con la Entidad.; el usuario debe seguir paso a paso el contenido del Manual del Usuario para Conexión por VPN.
- Se requiere que mientras se haga uso de VPN desde un equipo personal, éste tenga instalado y actualizado el antivirus y que el sistema operativo cuente con las actualizaciones de seguridad.
- El DETIC prohíbe cualquier otro tipo de acceso remoto y el uso de sistemas de información que no estén autorizados por el área de Tecnología.

La entidad cuenta con el Formato solicitud de usuarios VPN, el cual debe ser debidamente diligenciado por el solicitante y autorizado por el Subdirector de la ESDEG.

Servicios de Internet

La navegación en internet estará controlada de acuerdo con las categorías de navegación definidas para los usuarios; sin embargo, en ningún caso se consideran aceptable los siguientes usos:

- Navegación en sitio de contenido sexualmente explicito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.
- Publicaciones, envió o adquisición de material sexualmente explicito, discriminatorio o de cualquier otro contenido que se considere fuera de los límites permitidos.
- Publicación envió de información confidencial hacia fuera de la institución y entidades del sector defensa sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respetivos.
- Utilización de otros servicios disponibles a través de internet que permiten establecer conexiones o intercambio no autorizados.
- Publicación de anuncios comerciales o material publicitario, salvo las oficinas que dentro de sus funciones así lo requieran y estén autorizados de acuerdo con el Plan Estratégico de Comunicaciones.
- Promover o mantener asuntos o negocios personales.
- Descarga, instalación y utilización de programas de aplicación o software no relacionados con la actividad laboral y que afecte el procesamiento de la estación de trabajo o de la red.
- Navegación a las cunetas de correo de carácter personal, no institucional, o en redes sociales, sin una justificación por parte de la entidad.
- Uso de herramientas de mensajería instantánea no autorizadas.
- Emplear cuentas de correo externas no corporativas para él envió recepción de información institucional
- Se realizará monitoreo permanente de tiempo de navegación y páginas visitadas por los funcionarios y terceros autorizados. así mismo, se puede inspeccionar, registrar y e informar las actividades realizadas durante la navegación.
- El uso del internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información.

Computación en la nube: (cloud computing)

- Por ningún motivo se podrá almacenar información clasificada en servicios en la nube públicos o híbridos
- Ningún servicio de carácter operativo e institucional de la ESDEG deberá ser contratados en servicios en la nube público o híbridos.
- Para el caso de los procesos de educación, investigación y capacitación se podrá hacer uso de servicios en la nube públicos e híbridos, siempre y cuando no se vea comprometida la seguridad institucional o información clasificada
- La ESDEG, podrá implementar servicios de nube privada, a fin de hacer uso de las facilidades y bondades tecnológicas, garantizando la implementación de los controles adecuados.

Redes inalámbricas

- Se debe propender por la implementación y mantenimiento de ambientes de trabajo completamente independientes para la red operativa y la red con servicio de internet a fin de minimizar los riesgos de intrusión a las redes institucionales.
- Los usuarios de las redes inalámbricas deben ser sometidos a las mismas condiciones de seguridad de las redes cableadas en lo que respecta a identificación, autenticación, control de contenidos de internet y cifrado entre otros.
- El servicio de internet para formación y capacitación de los estudiantes y alumnos deberá contar con mecanismo de autenticación de usuarios y deberá estar configurado de tal manera que permita el desarrollo de las actividades académicas y de investigación
- Se debe implementar infraestructura inalámbrica que permite configuraciones de seguridad y en ningún caso se podrá dejar las configuraciones y contraseñas establecidas por defecto.

### 7.5.2 Política de gestión de acceso usuarios

Se deben establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.

Los procedimientos deben comprender todas las fases del ciclo de vida de acceso del usuario, desde el registro inicial de los usuarios nuevos hasta la cancelación final del registro de usuarios que ya no requieren acceso a los servicios y sistemas de información. Se debe poner atención a la asignación de derechos de acceso privilegiado, que permiten a los usuarios anular los controles del sistema.

7.5.2.1 Política registro y cancelación del registro de usuarios

El procedimiento de control de acceso para el registro y cancelación de registro de usuarios debe incluir:

- Uso de la identificación única de usuario (ID) para permitir que los usuarios queden vinculados y sean responsables de sus acciones; el uso de identificadores (ID) de grupo únicamente se debe permitir cuando son necesarios por razones operativas de la Institución, y deben estar aprobadas y documentadas.
- Verificación de que el usuario tenga autorización del dueño del sistema para el uso del sistema o servicio de información.
- Verificación de que el nivel de acceso otorgado sea adecuado para los propósitos de la Institución y que sea consistente con la política de Seguridad de la Información de la Institución, es decir, no pone en peligro la separación de funciones.
- Dar a los usuarios una declaración escrita de sus derechos de acceso.
- Exigir a los usuarios firmar declaraciones que indiquen que ellos entienden las condiciones del acceso.
- Asegurar que los proveedores del servicio no otorguen el acceso hasta que se hayan terminado los procedimientos de autorización.
- Mantener un registro formal de todas las personas autorizadas para usar el servicio.
- Retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado la Institución.
- Verificar, retirar o bloquear periódicamente las identificaciones (ID) y cuentas redundantes de usuarios.

- Garantizar que las identificaciones (ID) de usuario redundantes no se otorguen a otros usuarios.
- Se debe considerar la inclusión de cláusulas en los contratos del personal y de los servicios, que especifiquen las sanciones si el personal o los proveedores del servicio intentan el acceso no autorizado.

7.5.2.2 Política suministro de acceso de usuarios

El derecho de acceso otorgados a las identificaciones de usuario debe obedecer a:

- Obtener la autorización del propietario del sistema de información o del servicio para el uso del sistema de información o servicio.
- Verificar que el nivel de acceso otorgado es apropiado a las políticas de acceso y es coherente con otros requisitos, tales como separación de deberes.
- Asegurar que los derechos de acceso no estén activados antes de que los procedimientos de autorización estén completos.
- Mantener un registro central de los derechos de acceso suministrados a una identificación de usuario para acceder a sistemas de información y servicios.
- Adaptar los derechos de acceso de usuarios que han cambiado de roles o de empleo, y retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han dejado la organización.
- Revisar periódicamente los derechos de acceso con los propietarios de los sistemas de información o servicios.

7.5.2.3 Política gestión de derechos de acceso privilegiado

Los sistemas de usuario que requieren protección contra el acceso no autorizado deben controlar la asignación de privilegios a través de un proceso formal de autorización. Se deben tener en cuenta los siguientes elementos:

- Los privilegios de acceso asociados con cada producto del sistema, como sistema operativo, sistema de gestión de bases de datos y de aplicación, deben identificar a los usuarios que tienen acceso privilegiado.
- Los privilegios de administrador de cualquier equipo de cómputo (servidor, estación de trabajo, desktop, portátil, o equipo activo de red), deben ser asignados exclusivamente al Administrador del Sistema en DETIC. En ningún caso se deben asignar autorizar estos privilegios de acceso al usuario del equipo.
- Los privilegios se deben asignar a usuarios con base en la necesidad de utilizarlos y evento por evento, y de manera acorde con la política de control del acceso, es decir, el requisito mínimo para su función, sólo cuando sea necesario.
- Se debe conservar un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no se deben otorgar hasta que el proceso de autorización esté completo.
- Es conveniente promover el desarrollo y empleo de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.
- Se debe promover el desarrollo y empleo de programas que eviten la necesidad de funcionar con privilegios.
- Los privilegios se deben asignar a un identificador de usuario (ID) diferente a los utilizados para el uso normal del sistema.
- No se debe usar en el inicio de sesión de la red la contraseña de administrador, para evitar la intercepción de la contraseña en texto claro, que daría a un intruso acceso total al sistema.

7.5.2.4 Política gestión de información de autenticación secreta de usuarios

La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado, que incluya:

- Establecer la firma de una declaración para mantener confidencial la información de autenticación secreta personal; esta declaración firmada se puede incluir en los términos y condiciones del empleo para todos los usuarios.
- Estipular que todos los usuarios deben mantener su propia información de autenticación secreta, y se les suministra una autentificación secreta temporal segura, que se obligue a cambiar al usarla por primera vez.
- Establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle la nueva información de autenticación secreta de reemplazo o temporal.
- Definir que la información de autenticación secreta temporal se suministra a los usuarios de una manera segura; y se evitar utilizar partes externas o de mensajes de correo electrónico no protegidos (texto claro).
- Establecer que la información de autenticación secreta temporal es única para un individuo y no es fácil de adivinar.
- Definir que los usuarios deben acusar recibo de la información de autenticación secreta.
- Establecer que la información de autenticación secreta por defecto, del fabricante, se modifica después de la instalación de los sistemas o software.

7.5.2.5 Política revisión de los derechos de acceso de usuarios

El Oficial de Seguridad de la Información, debe revisar los derechos de acceso de los usuarios empleando un proceso formal que considere en la revisión los siguientes aspectos:

- Los derechos de acceso de los usuarios se deben revisar a intervalos regulares y modificar o reasignar estos derechos cuando se presenten cambios en el perfil de usuario, por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral.
- Se deben revisar las autorizaciones para derechos de acceso privilegiado a intervalos frecuentes para garantizar que no se tengan privilegios no autorizados o que no correspondan a las funciones del usuario.

7.5.2.6 Política retiro o ajuste de los derechos de acceso

Los derechos de acceso de todos los usuarios o partes interesadas a la información y a las instalaciones de procesamiento de información de la ESDEG se deben retirar al terminar su empleo, termino de contrato, traslado o pensión.; o se deben ajustar cuando se hagan cambios.

### 7.5.3 Política de responsabilidades de los usuarios

El usuario debe proteger los recursos asignados por la ESDEG, guardar el secreto de su contraseña, no prestar su clave de usuario bajo ninguna circunstancia.

El usuario debe hacer copias de seguridad de sus archivos importantes, borrar periódicamente sus correos y archivos no utilizados.

El usuario debe cambiar su contraseña periódicamente, de acuerdo con las políticas establecidas por el Administrador del Sistema.
El usuario debe notificar o informar al Oficial de Seguridad de la Información, cualquier novedad o incidente informático, que observe en el funcionamiento de su cuenta o en la aplicación de las políticas de Seguridad de la Información en los sistemas de información de la ESDEG.

7.5.3.1 Política uso de información de autenticación secreta

Se deberá exigir a los usuarios el uso de las buenas prácticas de seguridad de la organización en el uso de información confidencial para la autenticación, que incluye:

- Mantener la confidencialidad de la información de autenticación secreta, asegurándose de que no sea divulgada a ninguna otra parte, incluidas las personas con autoridad.
- Evitar llevar un registro (en papel, en un archivo de software o en un dispositivo portátil) de autenticación secreta, a menos que se pueda almacenar en forma segura y que el método de almacenamiento haya sido aprobado (una bóveda para contraseñas).
- Cambiar la información de autenticación secreta siempre que haya cualquier indicio de que se pueda comprometer la información.
- No compartir información de autenticación secreta del usuario individual.
- Establecer una protección apropiada de contraseñas cuando se usan éstas como información de autenticación secreta en procedimientos de ingreso automatizados, y estén almacenadas.
- No usar la misma información de autenticación secreta para propósitos de negocio y otros diferentes de estos.
- Definir que cuando se usa contraseñas como información de autenticación secreta, se debe seleccionar contraseñas seguras con una longitud mínima suficiente que:
  - Sean fáciles de recordar.
  - No estén basadas en algo que otra persona pueda adivinar fácilmente u obtener usando información relacionada con la persona, (nombres, números de teléfono y fechas de nacimiento, etc.).
  - No sean vulnerables a ataques de diccionario (es decir, no contienen palabras incluidas en los diccionarios).
  - estén libres de caracteres completamente numéricos o alfabéticos idénticos consecutivos.
  - sí son temporales, cambiarlos la primera vez que se ingrese.

### 7.5.4 Política control de acceso a sistemas y aplicaciones

El acceso lógico al software de aplicación y a la información debe ser restringido de acuerdo con el perfil del usuario.

Se debe suministrar protección contra acceso no autorizado por una utilidad del software del sistema operativo y software malicioso que pueda anular o desviar los controles del sistema o de la aplicación.

7.5.4.1 Política restricción de acceso a la información

- Se deben proporcionar menús para controlar el acceso a las funciones de los sistemas de aplicación.
- Se deben controlar los derechos de acceso de los usuarios, de manera particular, sobre cada uno de los sistemas, por ejemplo, leer, escribir, eliminar y ejecutar.
- Garantizar que los datos de salida de los sistemas de aplicación que manejan información sensible sean solo los solicitados y que se envían únicamente a terminales o sitios autorizados; esto debe incluir revisiones periódicas de dichas salidas para garantizar la seguridad de la información.

7.5.4.2 Política procedimiento de ingreso seguro

Se debe controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de inicio de sesión que incluya:

- No visualizar los identificadores del sistema o de la aplicación sino hasta que el proceso de ingreso se haya completado exitosamente.
- Visualizar una advertencia general acerca de que sólo los usuarios autorizados pueden acceder al computador.
- Evitar los mensajes de ayuda durante el procedimiento de ingreso, que ayudarían a un usuario no autorizado.
- Validar la información de ingreso solamente al completar todos los datos de entrada. ante una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta.
- Proteger contra intentos de ingreso mediante fuerza bruta.

- Llevar un registro con los intentos exitosos y fallidos.
- Declarar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de ingreso.
- No visualizar una contraseña que se esté ingresando.
- No transmitir contraseñas en un texto claro en una red.
- Terminar sesiones inactivas después de un período de inactividad definido, especialmente en lugares de alto riesgo tales como áreas públicas o externas por fuera de la gestión de seguridad de la organización o en dispositivos móviles.
- Restringir los tiempos de conexión para brindar seguridad adicional para aplicaciones de alto riesgo y para reducir la ventana de oportunidad para acceso no autorizado.
- Visualizar la siguiente información al terminar un ingreso seguro:

  • Registrar la fecha y la hora del ingreso previo exitoso.
  • Registrar los detalles de cualquier intento de ingreso no exitoso desde el último ingreso exitoso.

7.5.4.3 Política sistema de gestión de contraseñas

La asignación de contraseñas se debe controlar a través de un procedimiento formal de gestión y debe incluir como mínimo los siguientes requisitos:

- Se debe exigir a los usuarios la firma de una declaración para mantener confidenciales las contraseñas personales, esta declaración firmada se puede incluir en los términos y condiciones laborales.
- Cuando se exige a los usuarios mantener sus propias contraseñas, inicialmente se les debe suministrar una contraseña temporal segura que estén forzados a cambiar inmediatamente.
- Se deben establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle una contraseña temporal, de reemplazo o nueva.
- Las contraseñas temporales se deben suministrar de forma segura a los usuarios; se deben evitar mensajes de correo electrónico de terceras partes o sin protección (texto claro).
- Las contraseñas temporales deben ser únicas para un individuo y no descifrables.
- Los usuarios deben acusar el recibo de las contraseñas.
- Las contraseñas nunca se deben almacenar en sistemas de computador en un formato no protegido.
- Las contraseñas predeterminadas por el vendedor se deben cambiar inmediatamente después de la instalación de los sistemas o del software.

La creación, cambio y uso de las contraseñas para el acceso a las diferentes aplicaciones y sistemas de información de la ESDEG se debe hacer siguiendo las siguientes recomendaciones:

- Las contraseñas deben ser frases de mínimo ocho (8) caracteres de longitud, combinación de mayúsculas, minúsculas, caracteres especiales y números.
- Se deben configurar las políticas de claves, en los sistemas operativos cambiando la contraseña autoasignada regularmente (cada sesenta (60) días y con más frecuencia si se tienen privilegios de administrador) evitando reutilizar contraseñas antiguas.
- Siempre que se ingrese o digite la contraseña de acceso en el sistema se debe tener cuidado que no haya sido observado por otra(s) persona(s), si se tienen dudas hay que proceder a su cambio inmediato.
- No se deben escoger palabras del diccionario, palabras que estén relacionadas con el usuario (nombres propios, domicilio, fecha de nacimiento, etc.).
- Si se tiene más de una cuenta en distintos sistemas no es aconsejable utilizar la misma contraseña en todas.
- La contraseña es personal e intransferible, se debe mantener en sobre sellado y en custodia del jefe de cada Dependencia. Cuando por ausencia forzosa o retiro de algún funcionario, se requiera abrir el sobre sellado, esta será cambiada lo antes posible por el funcionario responsable.
- Mantener la confidencialidad de la contraseña (por ejemplo, no escribirla en un papel si no existe forma segura de guardarla), cambiar la contraseña si se tiene algún indicio o posibilidad de que su confidencialidad pueda verse comprometida.

- No incluir la contraseña en ningún procedimiento automático de conexión o que requiera un cambio de identificador de usuario (por ejemplo, en 'scripts' o 'guiones', macros, teclas de función, etc.).

Uso de cuentas sin contraseña por defecto

- Se deben Cambiar todas las contraseñas instaladas por defecto en el proceso de instalación del sistema operativo.
- Escanear el archivo de contraseñas periódicamente en busca de cuentas con UID igual a 0 (reservado para el usuario privilegiado de Administrador).
- Escanear el archivo de contraseñas en busca de cuentas nuevas de las que no se tiene conocimiento y que en la mayoría de los casos son indicativo de intrusión.
- No permitir la existencia de cuentas sin contraseña.
- Eliminar cuentas de usuarios que se hayan ido de la Institución y cuentas que no se estén utilizando.

Uso de contraseñas reusables

- Se debe reducir o eliminar la transmisión de contraseñas reusables en texto claro sobre la red, de esta forma se evita que las contraseñas sean capturadas por lo que se denomina packet sniffers (código para identificar contraseñas).

Uso de contraseñas de una sola vez

- Se debe utilizar el plan de cuentas del sistema, en la introducción de palabras clave para la validación de acceso autentificado. Se deben establecer algunos valores por defecto como son el número mínimo de caracteres que debe tener una contraseña, el máximo período de tiempo en el cual es válido, el mínimo período antes de que la contraseña sea cambiada, bloquear la cuenta después de tres inicios de sesión incorrectos.

Uso de cuentas de invitados (guest)

- Se debe evitar la existencia de cuentas de invitados "guest". En este sentido, muchos sistemas instalan cuentas para invitados por defecto, por lo que es necesario desactivar o eliminar del sistema este tipo de cuentas.
- Comprobar el archivo de contraseñas del sistema una vez haya terminado el proceso de instalación del sistema operativo a fin de asegurarse de que todas las cuentas predeterminadas tienen contraseñas válidas o han sido desactivadas o eliminadas

7.5.4.4 Política uso de programas utilitarios privilegiados

El uso de programas de utilidad que pueden ser capaces de anular los sistemas y los controles de aplicación se deben restringir al personal de DETIC, administradores de software y aquellos funcionarios que por la naturaleza de sus funciones requieran acceso.

Cuando se habilite el uso de programas utilitarios privilegiados por usuarios, se deben revisar como mínimo los siguientes aspectos:

- Segregación de programas de utilidad de software de aplicaciones
- Autorización para programas de utilidad Ad-hoc
- Eliminación o des habilitación de todos los programas de utilidad innecesarios.
- No dejar los programas de utilidad disponibles a los usuarios que tienen acceso a las aplicaciones de los sistemas donde se requiere la segregación de deberes.
- Política control de acceso a códigos fuente de programas

Las restricciones de acceso al código fuente de las aplicaciones software, deben incluir:

- Las librerías de fuentes de programas no se deben mantener en los sistemas operativos.
- El personal de soporte debe tener acceso restringido a las librerías de las fuentes de los programas.
- La actualización de las librerías de fuentes de programas y elementos asociados, y la entrega de fuentes de programas a los programadores sólo se deben hacer una vez que se haya recibido autorización por parte de DETIC.
- Los listados de programas se deben mantener en un entorno seguro.
- Conservar un registro de auditoría de todos los accesos a las librerías de fuentes de programas;
- Mantener y copiar las bibliotecas de fuentes de programas a través de procedimientos estrictos de control de cambios.

### 7.6 POLITICA CRIPTOGRAFIA

No se permite el uso de herramientas o mecanismos de cifrado de información diferentes a las autorizadas por el Ministerio de Defensa Nacional en cabeza del CITI, los cuales deben estar documentados en una lista de software autorizado que sea divulgada a todos los funcionarios y partes interesadas autorizadas.

#### 7.6.1 Política controles criptográficos

Se debe establecer el uso de controles criptográficos para la protección de la información.

Se debe establecer el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.

### 7.7. POLITICAS DE SEGURIDAD FISICA Y DEL ENTORNO

La ESDEG adoptará medidas para el control de acceso físico a las instalaciones y áreas seguras con el fin de mitigar los riesgos asociados a la afectación de la confidencialidad, disponibilidad e integridad de la información.

La ESDEG definirá áreas seguras y los controles de acceso físico correspondientes para la protección de la información que allí se resguarda.

Todas las personas que ingresen a las instalaciones de la ESDEG deben cumplir con los lineamientos establecidos para el control de acceso físico sin excepción.

#### 7.7.1 Política de áreas seguras

La implementación de medidas de seguridad física y de entorno, tiene como fin evitar el acceso físico no autorizado, el daño o la interferencia a las instalaciones y a la información de la organización.

Los servicios de procesamiento de información sensible o crítica deberán estar ubicados en áreas seguras o restringidas, protegidas por perímetros de seguridad definidos, con barreras de seguridad y controles de entrada adecuados. Dichas áreas deberán estar protegidas físicamente contra acceso no autorizado, daño e interferencia. La protección suministrada deberá estar acorde con los riesgos identificados.

7.7.1.1 Política perímetro de seguridad física

Se deberán utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjetas o dispositivos electrónicos o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información.

Se deberán considerar e implementar los siguientes aspectos para los perímetros de seguridad física:

- Se deben definir claramente los perímetros de seguridad y la ubicación y la fortaleza de cada perímetro deberá depender de los requisitos de seguridad, de los activos que protegen.
- Los perímetros de una edificación o un lugar que contenga servicios de procesamiento de información deben ser sólidos (es decir, no deberían existir brechas en el perímetro o las áreas en donde se podría producir fácilmente una violación de la seguridad); las paredes externas del sitio deberían tener una construcción sólida y todas las puertas externas deberán tener protección adecuada contra el acceso no autorizado con mecanismos de control tales como barras, alarmas, relojes, etc., las puertas y ventanas deberían estar cerradas con llave cuando no están atendidas y se debe tener presente la protección externa para las ventanas, particularmente a nivel del suelo.
- Se debe establecer un área de recepción atendida u otros medios para controlar el acceso físico al lugar o edificación, el acceso a los sitios y edificaciones deberá estar restringido únicamente al personal autorizado y cuando sea viable, se deben construir barreras físicas para evitar el acceso físico no autorizado.
- Si existen puertas contra incendio en el perímetro de seguridad, estas deben tener alarma, monitorearse y someterse a prueba junto con las paredes para establecer el grado requerido de resistencia, según las normas regionales, nacionales e internacionales; éstas deben funcionar de manera segura de acuerdo con el código local de incendios.
- Se deben instalar sistemas adecuados de detección de intrusos según normas nacionales, regionales o internacionales y someterlos a pruebas regularmente para cubrir todas las puertas externas y ventanas accesibles; las áreas desocupadas siempre deberán tener alarmas; también se debe tener cubrimiento de otras áreas, tales como los centros de cómputo y de comunicaciones.
- Las áreas de procesamiento de información clasificada o crítica de la organización deben estar físicamente separadas de aquellas dirigidas por terceras partes o personal externo.

7.7.1.2 Política controles de acceso físicos

- Las áreas críticas donde se administra información clasificada o crítica deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.
- Se debe establecer un control especial para el personal visitante y se debe llevar un registro que contenga: la fecha, la hora de entrada y salida de visitantes, sitio a visitar, motivo de la visita, persona que lo atiende y escolta, así como el nombre del funcionario que autoriza la visita. Todos los visitantes deberán estar supervisados y sólo se deben autorizar los accesos para propósitos específicos los cuales deben ser emitidos con instrucciones sobre los requisitos de seguridad del área y sobre los procedimientos de emergencia. De ser viable, se deberán incorporar dispositivos de cámaras, video o dispositivos biométricos.
- Se debe exigir a todos los funcionarios, contratistas y usuarios de terceras partes la utilización de alguna forma de identificación visible y se debe notificar inmediatamente al personal de seguridad si se encuentran visitantes sin acompañante y cualquiera que no use identificación visible.
- El acceso del personal de servicio de soporte o mantenimiento de terceras partes debe ser autorizado únicamente cuando sea necesario. Este acceso debe ser limitado para las áreas seguras o restringidas o a los servicios de procesamiento de información sensible y escoltado por un funcionario de la dependencia durante el tiempo de su permanencia. Se debe monitorear y registrar la actividad desarrollada.
- Las autorizaciones de acceso a áreas seguras o restringidas se deben revisar y actualizar con regularidad y revocar cuando sea necesario.

7.7.1.3 Política seguridad de oficinas, recintos e instalaciones

Se deben tener en cuenta los siguientes aspectos para la seguridad de oficinas, recintos y servicios:

- Aplicar los reglamentos y las normas pertinentes a la seguridad industrial y física de las instalaciones.
- Los servicios claves o sensibles se deben ubicar estratégicamente, de modo que se evite el acceso al público.
- Las edificaciones deben ser discretas y no tener indicaciones sobre su propósito. No deben tener señales obvias, fuera o dentro de ellas, que identifiquen a personas ajenas o visitantes, la presencia de actividades de procesamiento de información.

- Los directorios y los listados telefónicos internos que indican las ubicaciones y los servicios de procesamiento de información sensible no deben estar disponibles al público.

7.7.1.4 Política protección contra amenazas externas y ambientales

- Se deben tomar en consideración todas las amenazas de orden natural, humano, y tecnológico, de carácter fortuito o intencional, que afecten las instalaciones propias o circundantes, para diseñar y establecer los controles necesarios que garanticen la seguridad de las instalaciones propias.
- Los materiales combustibles o peligrosos, así como los suministros a granel tales como los materiales de oficina, deberán recibir un tratamiento especial para su almacenamiento, el cual debe ser en un área acondicionada que no afecte el área segura por explosión o conato de incendio.
- Las instalaciones con activos informáticos deben estar dotadas de equipos o sistemas apropiados contra incendios y tener diseños especiales para este fin.

7.7.1.5 Política trabajo en áreas seguras

Se deben tener en cuenta los siguientes aspectos de seguridad para trabajar en áreas seguras o restringidas.

- El personal sólo debe conocer las actividades que se desarrollan dentro de un área segura o restringida solo en función de su cargo o función asignada.
- El trabajo en áreas seguras o restringidas debe ser supervisado permanentemente para evitar las oportunidades de actividades maliciosas.
- Las áreas seguras o restringidas vacías deberán tener bloqueo físico y se deben revisar periódicamente.
- En las áreas seguras o restringidas no se debe permitir el acceso con equipos de cómputo o equipos electrónicos tales como videograbadoras, cámaras fotográficas, celulares, dispositivos de almacenamiento, equipos de transmisión o recepción de señales u otros dispositivos que puedan vulnerar la seguridad del área y activos informáticos.

7.7.1.6 Política áreas de despacho y carga

- Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se deben controlar y aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.
- El área de despacho y carga se debe ubicar de tal forma que los suministros se puedan descargar sin que el personal de despacho tenga acceso a otras partes de la edificación.
- Las puertas externas del área de despacho y entrega deben estar aseguradas mientras las puertas internas estén abiertas.
- El material que llega se debe inspeccionar para determinar posibles amenazas antes de moverlo desde el área de despacho y carga hasta el punto de uso.
- El material que llega se debe registrar de acuerdo con los procedimientos de gestión de activos a su entrada al lugar.
- Los envíos entrantes y salientes se deben separar físicamente, cuando sea posible.

**7.7.2 Política equipos**

Sobre los equipos más críticos de la red se deben definir políticas de arranque del sistema tales como contraseña de la configuración. Adicionalmente considerar la implementación de sistemas de autenticación basados en sistemas biométricos, de acuerdo con lo crítico de la función del PC en la red y del personal que valide su acceso a través de este.

Se debe limitar el uso de los recursos compartidos, de ser necesario se deben habilitar los mecanismos de control en el sistema para dar acceso a usuarios autorizados.

Los equipos que almacenen información clasificada y/o sensible, no deben tener salida a Internet y aplicar las políticas de seguridad para manejo de información establecidas.

7.7.2.1 Política ubicación y protección de los equipos

Los equipos que hacen parte de la infraestructura tecnológica deben ser ubicados y protegidos adecuadamente para prevenir la perdida, daño, robo, o acceso no autorizado de los mismo.

- Los equipos deben tener instalado y actualizado el antivirus y software de seguridad como antispam, antispyware, antikeyloggers, firewall personal, para evitar perdida de información y daños en el sistema del equipo.
- Adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética vandalismo entre otros.
- Los funcionarios y terceros velarán por el uso adecuado de los equipos de escritorio, portátiles, móviles que les hayan sido asignados, por lo tanto, dichos equipos no deberán ser prestados a personas ajenas o no autorizadas
- Los equipos tales como máquinas de copiado, impresoras y máquinas de fax deberán estar ubicados en zona de acceso restringido y se permitirá el uso a personal autorizado.
- Los equipos portátiles deberán estar asegurados (cuando este desatendidos) con la guaya o el mecanismo que se defina para su protección, sea dentro o fuera de las instalaciones de la ESDEG.
- Se deben asegurar las partes físicas de los equipos y periféricos, sobre el escritorio en el caso que estos equipos sean críticos para la red.

Los usuarios y partes interesadas deben acatar las siguientes recomendaciones en lo relacionado con los recursos tecnológicos:

- La instalación de cualquier tipo de software en los equipos de cómputo de la ESDEG es responsabilidad exclusiva de DETIC, por tanto, son los únicos autorizados para realizar esta labor.
- Ningún activo de información debe ser instalado con la configuración establecida por defecto por el fabricante o proveedor, incluyendo cuentas y claves de administrador.
- Los usuarios no pueden realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla no definido, estos cambios pueden ser realizados únicamente por DETIC.
- Los usuarios no deben realizar cambio físico en las estaciones de trabajo, tales como, cambio de ubicación, mantenimientos, repotenciación, modificación en su configuración física. estas actividades solo podrán ser realizadas por DETIC.
- Los equipos de cómputo asignados deben ser devueltos a la dependencia responsable una vez sean reemplazados o cuando el funcionario o tercero responsable de dicho equipo finalice su vinculación con la entidad.
- De acuerdo con el literal anterior, las dependencias no deben almacenar equipos de cómputo en las oficinas una vez haya cesado el uso de los mismos.

7.7.2.2 Política servicios de suministro

Todos los servicios de soporte, tales como electricidad, suministro de agua, alcantarillado, calefacción / ventilación y aire acondicionado deben ser adecuados para los sistemas a los que dan apoyo.

- Los servicios de soporte se deben inspeccionar regularmente y someter a las pruebas apropiadas para garantizar su efectividad y reducir los riesgos de mal funcionamiento y falla.
- Se debe proporcionar un suministro eléctrico acorde con las especificaciones del fabricante del equipo.
- Se debe tener un suministro de energía sin interrupción (UPS) para dar soporte al cierre ordenado o al funcionamiento continuo de equipos que soportan operaciones críticas.

- Los planes de contingencia deben incluir la acción que se ha de tomar en caso de falla de la UPS. Se recomienda pensar en un generador de soporte, si se requiere la continuidad del procesamiento en caso de fallas energéticas prolongadas.
- Se debe tener disponible el suministro adecuado de combustible para garantizar que el generador pueda funcionar por un periodo prolongado. El equipo de UPS y los generadores se deben revisar con regularidad para asegurarse de que tienen la capacidad adecuada y someterse a prueba según las recomendaciones del fabricante.

7.7.2.3 Política seguridad del cableado

- El cableado de energía eléctrica y estructurado debe cumplir con las normas técnicas actuales aplicables.
- El cableado de la red debe estar protegido contra interceptación no autorizada o daño, utilizando conductos rutas a través de áreas públicas.
- Los cables de energía deben estar separados de los cables de comunicaciones para evitar interferencia.
- Se debe utilizar rótulos de equipo y de cables claramente identificables para minimizar los errores en el manejo, tales como conexiones provisionales de cables erróneos en la red.
- Se debe emplear una lista de las conexiones temporales documentadas para reducir la posibilidad de errores.
- Para sistemas críticos o sensibles se deben tener controles adicionales incluyendo:

  - Instalación de conductos blindados y recintos o cajas bloqueadas en los puntos de inspección y terminación.
  - Uso de medios alternos de enrutamiento y/o transmisión que suministren seguridad adecuada.
  - Uso de cableado de fibra óptica.
  - Uso de pantallas electromagnéticas para proteger los cables.
  - Inicio de reconocimientos técnicos e inspecciones para detectar dispositivos no autorizados ajustados a los cables.
  - Acceso controlado a los paneles o racks y a recintos de cables.

7.7.2.4 Política mantenimiento de equipos

- El mantenimiento, modificación o cualquier tipo de arreglo a los equipos de cómputo, periféricos, debe ser realizado únicamente por personal autorizado, bajo la supervisión del usuario.
- Al final del trabajo debe quedar copia del informe técnico respectivo. Cualquier novedad debe ser reportada al administrador de los servicios informáticos de la unidad.
- Se debe asegurar que, sobre la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la Seguridad de la Información, se realicen mantenimientos periódicos con el fin de que dichas actividades no se vean afectadas por obsolescencia. por lo tanto, revisara constantemente la vida útil de cada uno de los recursos que componen dicha infraestructura de acuerdo con la descripción y recomendaciones de sus fabricantes
- La ESDEG debe procurar la adquisición de pólizas o seguros para la reposición de los activos informáticos que respalda los planes de contingencia y la continuidad de los servicios.
- Los discos duros dañados o para reparación no pueden salir de las instalaciones.

7.7.2.5 Política retiro de activos

- Los equipos de cómputo que contengan información clasificada y/o sensible pueden ser retirados de su sitio original, para mantenimiento correctivo, teniendo en cuenta que las unidades de almacenamiento de este equipo deben ser retiradas del equipo, y guardadas de forma segura por el usuario responsable mientras dure el proceso de mantenimiento. Estos procedimientos deben tener autorización del jefe de la Dependencia. En todos los casos, es necesario informar a la Dependencia o persona encargada de los inventarios fiscales.
- Si por razones de trabajo los funcionarios que tengan a su cargo un equipo de cómputo necesitan llevarlo a sitios fuera de las instalaciones, deben estar previamente autorizados por el jefe de la Dependencia, y

la información sensible y clasificada que contengan, debe estar encriptada en el disco duro y/o borrada en forma segura. Estos funcionarios deben aplicar todas las políticas de seguridad establecidas para estos casos

- Se deben establecer límites de tiempo para el retiro de equipos y verificar el cumplimiento y registro en el momento de devolución.
- Los controles al azar se deben realizar para determinar el retiro no autorizado de propiedad, también se pueden usar para detectar dispositivos de grabación no autorizados, armas, etc., y evitar su ingreso. Tales controles al azar se deben llevar a cabo según los planes de Contrainteligencia de cada unidad.

7.7.2.6 Política seguridad de equipos y activos fuera de las instalaciones

- Los usuarios que requieran manipular los equipos o medios fuera de las instalaciones de la ESDEG deben velar por la protección de los mismos sin dejarlos desatendidos comprometido la imagen o información del sector.
- El propietario del activo, con el apoyo de DETIC, identificará mediante una metodología de análisis de riesgo que establezca, los riesgos potenciales que pueda generar el retiro de equipos o medio de las instalaciones; así adoptará los controles necesarios para la mitigación de dichos riesgos.
- En caso de pérdida o robo de un equipo portátil, o cualquier medio que tenga información relacionada con la defensa con la seguridad nacional, se deberá realizar inmediatamente el reporte de acuerdo con el procedimiento gestión de incidentes de seguridad y se deberá poner la denuncia ante la autoridad competente, si aplica.
- Los equipos de cómputo o activos de información que por razones de servicio se retiren de las instalaciones de la ESDEG, deberán contener únicamente la información estrictamente necesaria para el cumplimiento de su misión y se deshabilitaran los recursos que no se requieren o que puedan poner en riego la información que contiene.

7.7.2.7 Política disposición segura o reutilización de equipos

- Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que no se haya eliminado algún software con licencia ni datos sensibles o asegurar que se hayan sobrescrito con seguridad antes de la eliminación.
- Los dispositivos que contienen información sensible se deben destruir físicamente o su información se debe destruir, borrar o sobrescribir usando técnicas que permitan que la información original no se pueda recuperar, en lugar de utilizar las funciones de borrado o formateado estándar.
- Los dispositivos deteriorados que contengan datos sensibles se les debe hacer una evaluación de riesgos para determinar si los elementos se deben destruir físicamente en lugar de enviarlos a reparación o desecharlos.

7.7.2.8 Política equipos de usuario desatendidos

- Los usuarios deben asegurarse de que los equipos desatendidos tengan protección apropiada y responsabilizarse de la implementación de dicha protección.
- Se deben cerrar las sesiones activas cuando finalice el trabajo, a menos que se puedan asegurar por medio de un mecanismo de bloqueo, como un protector de pantalla protegido por contraseña.
- Se debe realizar el registro de cierre en computadoras principales, servidores y computadores personales de oficina al terminar la sesión (es decir, no sólo apagar el interruptor de la pantalla del computador o terminal).
- El usuario debe cancelar todas las sesiones activas antes de dejar el equipo desatendido, salvo si se dispone de una herramienta de bloqueo general. El equipo debe tener configurada la opción de protector de pantalla con contraseña, con un tiempo mínimo de activación.
- El usuario debe desconectarse (Log-off) de todas las sesiones con los servidores antes de apagar el equipo. Los equipos de los usuarios deben quedar apagados al término de labores.

7.7.2.9 Política de escritorio limpio y pantalla limpia

- No deberán dejarse documentos críticos en el "Escritorio" tanto físico como el Escritorio virtual (se denomina "Escritorio" al espacio digital en los equipos de cómputo).
- En horas no hábiles o cuando los sitios de trabajo se encuentren desatendido, los usuarios deberán dejar los medios que contengan información crítica protegida bajo llave.
- Los usuarios deberán bloquear su estación cada vez que se retiren de su puesto de trabajo y solo se podrá desbloquear con la contraseña del mismo usuario que la bloqueo.
- Todas las estaciones de trabajo deberán usar únicamente el papel tapiz y el protector de pantalla establecido y el logo de ADVERTENCIA DE USO para manejo de los recursos informáticos Institucionales.
- Los usuarios no deberán almacenar en el escritorio de sus estaciones de trabajo documentos, accesos directos a los mismos o a sistemas de información sensibles
- Los usuarios son responsables por la custodia y las acciones que se realicen a través de los activos informáticos asignados, por consiguiente deben estar presentes en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización de dichos activos.

## 7.8 POLITICA SEGURIDAD DE LAS OPERACIONES

Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación de la ESDEG. La ESDEG planea, gestiona, respalda y monitorea la infraestructura tecnológica siguiendo los lineamientos establecidos en los procedimientos establecidos para el SGSI.

### 7.8.1 Política procedimientos operacionales y responsabilidades

7.8.1.1 Política procedimientos de operación documentados

Los procedimientos operativos deben especificar las instrucciones para la ejecución detallada de cada trabajo, teniendo en cuenta:

- Procesamiento y manejo de información.
- Copias de respaldo.
- Requisitos de programación, incluyendo las interdependencias con otros sistemas, hora de comienzo del trabajo inicial y de terminación del trabajo final.
- Instrucciones para el manejo de errores y otras condiciones excepcionales que se pueden presentar durante la ejecución del trabajo, restricciones al uso de las utilidades del sistema.
- Contactos de soporte en caso de dificultades técnicas u operativas inesperadas.
- Instrucciones de manejo de los medios y los resultados especiales, como el uso de papelería especial o el manejo de los resultados confidenciales incluyendo los procedimientos para la eliminación segura de los resultados de trabajos fallidos.
- Procedimientos para el reinicio y la recuperación del sistema que se deben usar en caso de falla del sistema.
- Gestión de la prueba de auditoría y de la información de registro del sistema.
- Los procedimientos operativos y documentados para las actividades con los activos informáticos de la ESDEG deben tratarse como documentos formales y sus cambios deben ser autorizados por los responsables de cada área de trabajo.

7.8.1.2 Política gestión de cambios

Los sistemas operativos y el software de aplicación deben estar sujetos a un control sólido de la gestión del cambio, se deben considerar los siguientes elementos:

- Identificación y registro de los cambios significativos.
- Planificación y pruebas de los cambios.
- Evaluación de los impactos potenciales de tales cambios, incluyendo los impactos en la seguridad.
- Procedimiento de aprobación formal para los cambios propuestos.
- Comunicación de los detalles del cambio a todos los usuarios involucrados.

- Procedimientos de emergencia, incluyendo los procedimientos y las responsabilidades de cancelar o recuperarse de cambios fallidos y eventos imprevistos.
- Los cambios en los sistemas operativos sólo se deben realizar cuando existe una razón válida para la Institución.

7.8.1.3 Política gestión de capacidad

- Se debe hacer seguimiento y adaptación del uso de los recursos informáticos, así como proyecciones de los requisitos de capacidad futura para asegurar el desempeño requerido de los sistemas de la ESDEG.
- Se debe poner atención a los recursos cuya adquisición toma mucho tiempo o requiere costos elevados; por lo tanto, el oficial de Seguridad de la Información debe monitorear la utilización de los recursos claves de los sistemas.
- Se deben identificar las tendencias del uso, particularmente en relación con las aplicaciones de la Institución o las herramientas del sistema de información para la gestión Institucional.

7.8.1.4 Política separación de los ambientes de desarrollo, pruebas y operación

Se deben separar los ambientes operativos, de prueba y de desarrollo, para prevenir problemas operativos e implementar los controles adecuados, teniendo en cuenta los siguientes aspectos:

- Definir y documentar las reglas para la transferencia de software del estado de desarrollo al operativo.
- El software de desarrollo y el operativo se debe ejecutar en diferentes sistemas o procesadores de computación y en diferentes dominios o directorios.
- Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no deben ser accesibles por usuarios no autorizados.
- El ambiente del sistema de prueba debe emular el ambiente del sistema operativo lo más estrechamente posible.
- Los usuarios deben emplear perfiles de usuario diferentes para los sistemas operativos y de prueba y los menús deben desplegar mensajes de identificación adecuados para reducir el riesgo de error.
- Los datos sensibles no deben ser copiados en el entorno del sistema de prueba.

Cuando el personal de desarrollo y de pruebas tiene acceso al sistema operativo y a la información, pueden introducir códigos no autorizados sin probar o alterar los datos operativos. En algunos sistemas, esta capacidad podría ser mal utilizada para cometer fraude o introducir códigos maliciosos o sin probar, lo cual puede crear problemas operativos graves.

### 7.8.2 Política protección contra códigos maliciosos

La protección contra códigos maliciosos se debe basar en software de detección y reparación de daños por códigos maliciosos.

7.8.2.1 Política controles contra códigos maliciosos

- Se deben realizar revisiones regulares del software y del contenido de datos de los sistemas que dan soporte a los procesos críticos de la Institución,
- Se debe investigar la presencia de archivos no aprobados o parches no autorizados en el sistema.
- Se debe verificar la presencia de códigos maliciosos en todos los archivos, medios ópticos o electrónicos y archivos recibidos en las redes antes de su uso.
- Se debe verificar la presencia de códigos maliciosos en los adjuntos y las descargas del correo electrónico antes del uso; esta verificación se debe efectuar en diferentes lugares, como servidores de correo electrónico, los computadores de escritorio y cuando ingresan a la red de la Institución.
- No se deben visitar, consultar y descargar archivos de páginas Web de dudosa procedencia.
- Se deben definir responsabilidades y procedimientos de gestión para tratar la protección contra códigos maliciosos, la formación sobre su uso, el reporte y la recuperación debido a ataques de códigos maliciosos.

- Se deben preparar planes adecuados para la continuidad operativa de la Institución con el fin de recuperarse de los ataques de códigos maliciosos, incluyendo todos los datos y el soporte de software necesario y las disposiciones para la recuperación.
- El Oficial de Seguridad de la Información debe implementar los procedimientos para recolectar información con regularidad, como la suscripción a sitios Web de verificación y / o listados de correo que suministren información sobre los códigos maliciosos nuevos.
- Los antivirus se deben controlar en los servidores como en las estaciones de trabajo.

Así mismo, Se deben tener en cuenta las siguientes consideraciones para la protección contra códigos móviles que ejecutan acciones no autorizadas:

- Cuando se va a trabajar en un entorno con códigos móviles, se debe identificar el código móvil y la función o servicio que ejecuta en el software personalizado y ejecutarlo en un entorno con aislamiento lógico para verificar su funcionamiento correcto y su autenticidad con técnicas de hash.
- Se debe bloquear el sistema para que no ejecute o use o reciba cualquier código móvil.
- Se deben controlar los recursos disponibles para el acceso de los códigos móviles.
- Los controles criptográficos sirven para autenticar de forma única el código móvil.

### 7.8.3 Política copias de respaldo

Se debe preservar la integridad y disponibilidad de la información y de los servicios de procesamiento de información, para lo cual se debe tener en cuenta tanto para el hardware como el software, los siguientes aspectos:

7.8.3.1 Política respaldo de la información

Se deben considerar los siguientes elementos para el respaldo de la información:

- Definir el nivel necesario para la información de respaldo.
- Se deben hacer registros exactos y completos de las copias de respaldo y los procedimientos documentados de restauración.
- La frecuencia de los respaldos debe reflejar los requisitos de seguridad de la información involucrada y la importancia de la operación continua de la Institución.
- Los respaldos se deben almacenar en un sitio lejano apropiado con protección física, lógica y ambiental, a una distancia suficiente para escapar a cualquier daño debido a desastres en la unidad principal.
- Los procedimientos de restauración tanto como los medios de respaldo se deben verificar y probar con regularidad para garantizar su eficacia y que se pueden completar dentro del tiempo designado en los procedimientos operativos para la recuperación en caso de contingencia o desastre. Se debe designar a una persona como operario de copias de respaldo de los servidores de red y Bases de Datos de la ESDEG; esta persona será la encargada de realizar esta labor en las horas no hábiles de la Institución, con el fin de independizar este proceso de los administradores de los sistemas, quienes solo designarán a qué segmentos de sus máquinas se realizarán dichas copias. Este operador debe tener acceso de operador (solamente) a los sistemas operativos con el fin de realizar su labor.

### 7.8.4 Política registro y seguimiento

Tanto los sistemas de información que manejan información crítica, como los dispositivos de procesamiento, de red, y de Seguridad de la Información deberán general registro de eventos que serán verificados periódicamente con el fin de detectar actividades no autorizadas sobre la información, siguiendo el procedimiento monitoreo y revisión de “Logs”.

El tiempo de retención de los “logs” estará dado por las condiciones específicas de cada sistema de información, recurso informático o dispositivo de red y por las leyes, normativas o regulaciones que rigen al sector defensa.

El lugar de retención de los registros está definido por el nivel de clasificación de información que posean dichos registros.

7.8.4.1 Política registro de eventos

Todo aquel evento que se identifique por medio del monitoreo y revisión de los registros y que ponga en riesgo la integridad disponibilidad o confidencialidad de la infraestructura tecnológica deberá ser reportado a DETIC mediante el procedimiento de gestión de incidentes de seguridad.

- Los registros de eventos de la red de la ESDEG deben ser revisados por el Administrador del Sistema y el Oficial de Seguridad de la Información, sobre una base mensual o eventual ante la presencia o sospecha de incidentes informáticos.
- Todos los registros de auditoria serán mantenidos en archivo por un período de 12 meses para revistas y como referencia.
- Los registros de eventos deben indicar el momento exacto y el usuario (persona o proceso) que lo realizó, para garantizar que la información relacionada con las acciones y actividades de los usuarios se encuentre debidamente registrada y monitoreada.

Registro de fallas

- Se deben registrar las fallas reportadas por los usuarios o por los programas del sistema relacionadas con problemas de procesamiento de la información o con los sistemas de comunicación.
- Se deben revisar los registros de fallas para garantizar que éstas se han resuelto satisfactoriamente.
- Se deben registrar las medidas correctivas para garantizar que no se han puesto en peligro los controles y que la acción tomada está totalmente autorizada.
- Se debe asegurar que el registro de errores está habilitado, si esta función del sistema está disponible.

7.8.4.2 Política protección de la información de registro

- Se deben instalar sistemas de monitoreo de la red, detección de intrusos y detección de vulnerabilidades para realizar labores encaminadas a obtener información respecto al uso de la red, rendimiento, acceso a los sistemas y detectar posibles ataques al sistema y la forma de realizarlos.
- Se debe llevar un registro de la administración de configuración de todo el equipo (hardware, software, soporte lógico inalterable –firmware-, interfaces de comunicaciones, procedimientos de funcionamiento y estructuras de la instalación).
- Incluido en el expediente de administración de la configuración y un listado detallado de todos los cambios temporales a los lineamientos aprobados de la red.
- Se debe llevar un registro de todo el mantenimiento y reparaciones del hardware de la red de la ESDEG, incluyendo la instalación o el retiro de los equipos activos y de sus dispositivos, así como un registro de todos los visitantes autorizados y un registro de los chequeos de seguridad realizados y el comienzo y cierre de cada día de trabajo.

7.8.4.3 Política registros del administrador y del operador

Se debe establecer un perfil y registro de las personas que operan los sistemas y el operador de backups de los servidores, con el fin de determinar la confiabilidad de estas personas. Es importante que las personas que integren este grupo sean personas que estén amparadas bajo cláusulas de confidencialidad.

7.8.4.4 Política sincronización de relojes

Se debe implementar un servidor de sincronización de tiempo para todos los equipos activos de la red de la ESDEG. Esta sincronización debe ser verificada periódicamente por el Oficial de Seguridad de la Información.

### 7.8.5 Política control de software operacional

7.8.5.1 Política instalación de software en sistemas operativos

- La actualización del software operativo, las aplicaciones y las librerías de los programas sólo se debe realizar por administradores capacitados.
- Los sistemas operativos únicamente deben contener códigos ejecutables aprobados.
- El software de las aplicaciones y del sistema operativo sólo se deben implementar después de pruebas de funcionabilidad y de tiempos de respuesta.
- Se debe usar un sistema de control de configuración. para mantener el control del software implementado, así como de la documentación del sistema.
- Se debe conservar un registro para auditoria de todas las actualizaciones de las librerías de los programas operativos.
- Es conveniente conservar las versiones anteriores del software de aplicación como medida de contingencia.
- Las versiones antiguas de los aplicativos se deben archivar junto con toda la información requerida y los parámetros, procedimientos, detalles de configuración y software de soporte, en la medida en que los datos se retengan en archivo.
- Ningún software debe estar en producción sin soporte y se debe prever que en la contratación quede establecida la transferencia tecnológica.
- El acceso físico o lógico únicamente se debe dar a los proveedores para propósitos de soporte, cuando sea necesario, y con la respectiva aprobación. Las actividades del proveedor se deben monitorear.

### 7.8.6 Política gestión de la vulnerabilidad técnica

7.8.6.1 Política gestión de las vulnerabilidades técnicas

- El DETIC se encargará de identificar las vulnerabilidades técnicas de las diferentes plataformas tecnológicas y para esto definirá las herramientas y/o servicios necesarios.
- El DETIC se encargará de proponer y ejecutar un programa de evaluación y gestión de vulnerabilidades que debe ser utilizado para la plataforma técnica de la institución o entidad.
- No se permite a los usuarios de los activos informáticos sin la autorización expresa de DETIC, realizar o participar por iniciativa propia o de los terceros, en pruebas de acceso o ataques activos o pasivos a los activos informáticos, o a la actualización de los mismos para efectuar pruebas de vulnerabilidades o ataques a otros equipos o sistemas externos.
- Los administradores de la plataforma y sistema de información serán responsables de mantener protegida la infraestructura a su cargo de los riesgos derivados de vulnerabilidades técnicas e identificadas.
- EL DETIC realizara las revisiones de las alertas de seguridad definiendo en caso de ser negociable para mitigar el impacto de las mismas en los ambientes de producción y desarrollo de la infraestructura tecnológica.

7.8.6.2 Política restricciones sobre la instalación de software

La instalación de cualquier tipo de software en los equipos de cómputo de la ESDEG es responsabilidad exclusiva de DETIC, por tanto, son los únicos autorizados para realizar esta labor.

## 7.9 POLITICAS DE SEGURIDAD EN LAS COMUNICACIONES

El DETIC, establecerá los controles para acceso lógico y protección de las redes de la ESDEG, con el fin de asegurar y cumplir con los acuerdos de niveles de servicios que sean establecidos para los servicios de red y que deberán ser acordados con la alta dirección.

La ESDEG definirá procedimientos y lineamientos para la transferencia segura de información interna o externamente, de tal forma que se garantice la integridad y confidencialidad de la información.

### 7.9.1 Política gestión de la seguridad de las redes

Las redes de la ESDEG se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.

7.9.1.1 Política controles de redes

El administrador de red y el Oficial de Seguridad de la Información deben implementar controles que garanticen la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado.

Se deben tener en cuenta los siguientes elementos:

- La responsabilidad operativa por las redes debe estar separada de las operaciones del computador.
- Es necesario establecer las responsabilidades y los procedimientos para la gestión de equipos remotos, incluyendo los equipos en áreas de usuarios.
- Se deben establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan por redes públicas o redes inalámbricas y para proteger los sistemas y las aplicaciones conectadas, también se deben tener controles especiales para mantener la disponibilidad de los servicios de la red y los computadores conectados.
- Se debe aplicar el registro y el monitoreo adecuado, para permitir el registro de acciones de seguridad pertinentes.
- Se deben coordinar actividades de gestión para optimizar el servicio de la Institución y para garantizar que los controles se aplican consistentemente en toda la infraestructura del procesamiento de información de la ESDEG.

7.9.1.2 Política seguridad de los servicios de red

Switches

- Se deben activar todas las opciones de seguridad del Switch y deshabilitar todos los servicios del Switch que no se van a usar tales como TFTP para un cliente remoto.
- La configuración del Switch solo se debe realizar localmente, o en su defecto designar mediante listas de control de acceso (ACL) a un IP único remoto, asociado a la Mac de la estación remota.

Enlaces de redes

- Se debe tener un control del personal que se comunica con redes externas (Internet, Intranet, Extranet), así como clasificar el tipo de información a intercambiar entre las entidades interconectadas.
- Se deben documentar todas las comunicaciones con entidades externas a través de accesos conmutados, dedicados o públicos, teniendo en cuenta los equipos activos, medio de comunicación, direcciones IP y diagramas de conexión Ni FTP Ni TELNET: deben ser usados para transferencia de datos y apertura de sesión remota. En su lugar se debe utilizar SFTP para transferir archivos, SSH con ciframiento para emulación de terminales, tanto al interior de las unidades como en la Intranet.

Implementación y encriptación sobre los enlaces

- La comunicación con entidades internas y externas a través de accesos dedicados, conmutados o públicos deben ser encriptados.
- Se debe implementar un sistema de detección de intrusos IDS dentro de la red, con el fin de detectar cualquier tipo de actividad contra los sistemas presentes.
- Se debe mantener un sistema único de identificación de direcciones IP fijos para cada equipo. No es recomendable el uso de DHCP para validación de trazas y registros de auditoria.

Comunicación remota

- Se deben restringir al máximo los recursos que se van a autorizar a los usuarios remotos, se debe contar con sistemas de autenticación fuertes para dichos accesos.
- En el caso que sea necesario compartir grandes volúmenes de datos a través de estas conexiones, se deben implementar redes privadas virtuales VPN, con el fin de garantizar la integridad de la comunicación y sistemas de detección de intrusos IDS para cada conexión. Se deben tener en cuenta reglas de autenticación para evitar posibles ataques.
- Cuando se realicen comunicaciones remotas a través de antenas parabólicas para transmisión vía satélite, o conexiones inalámbricas, éstas se deben instalar o ubicar en un sitio especialmente protegido, con base en las recomendaciones del fabricante, teniendo en cuenta las medidas de seguridad necesarias.

Firewall

- En la instalación y configuración inicial de firewalls, se debe partir del principio que todos los servicios y puertos están negados y cerrados, a menos que expresamente sean habilitados y abiertos según el diseño preestablecido para la red.
- Se deben configurar las reglas del Firewall, de acuerdo con los servicios que se necesiten, además se deben tener presentes los puntos vulnerables de toda la red, los servicios que se disponen como públicos al exterior de ella (WWW, FTP, TELNET, entre otros) y conexiones por modem (dial-up modem calling) o conexiones inalámbricas.
- Este elemento debe mantener un control de las conexiones provenientes del interior y exterior de la ESDEG a las redes internas y viceversa. Garantizando la autenticación y autorización.

Monitoreo, sistemas de detección de intrusos (IDS) y de vulnerabilidades

- La red debe ser monitoreada de manera permanente y se deben instalar sistemas de detección de intrusos en todos los puntos críticos de la red, para detectar posibles ataques o incidentes informáticos.
- Se deben hacer análisis de vulnerabilidades a la red, documentar los resultados y tomar las acciones correctivas a que haya lugar.

Virtual Private Network (VPN)

- Las comunicaciones que se establezcan entre usuarios externos y la red interna deben hacerse a través de un canal virtual privado que permita establecer una comunicación segura, garantizando los siguientes fundamentos de autenticación, confidencialidad e integridad.

Secure Socket Layer (SSL)

- Cuando se ingrese a sitios que utilicen el protocolo SSL, el usuario debe verificar que el certificado sea válido, para acceder o enviar información con seguridad.

Seguridad a nivel de servidores

- Los servidores deben cumplir con los servicios de auditoría, reuso de objetos y debe existir un Administrador del Sistema con cuenta en cada uno de los servidores y será independiente del Oficial de Seguridad de la Información.

Servidores de red

- Se debe estudiar periódicamente la información contenida en los discos del servidor, a qué usuarios pertenece, prioridades, distribución de usuarios, grupos de usuarios, derechos de usuarios, políticas de cuentas, claves de acceso y auditar todos los procesos: (ingresos al sistema, intentos de accesos fallidos, fallas en entrada al sistema).

Servidores WEB

- Los Servidores Web deben ser administrados por el grupo técnico correspondiente. La edición y contenido de la información de dicho servidor quedará bajo responsabilidad de la persona que procese y administre la información y contenido del mismo.
- El servidor Web que permita el acceso a Bases de Datos desde la red pública (Internet) debe estar registrado y autenticado ante una unidad certificadora. Los Servicios Web deben basarse en SOAP, UDDI y WDSL

Listas de Control de Acceso (ACL)

- Las listas de control de acceso deben estar configuradas en los equipos de comunicaciones asociadas en una tabla, de manera que los usuarios y/o redes en ella registrados, son los que el sistema autoriza o niega el acceso.

7.9.1.3 Política separación en las redes

- Se deben separar los grupos de servicios de información, usuarios y sistemas de información, por dominios de red internos y dominios de red externos, cada uno protegido por un perímetro de seguridad definido, aplicando un conjunto graduado de controles en los diferentes subdominios.
- La separación de las redes se debe basar en el valor y la clasificación de la información almacenada o procesada en la red, los niveles de confianza o los lineamientos de la red con el fin de reducir el impacto total de una interrupción del servicio.
- Se deben separar las redes inalámbricas procedentes de redes internas y/o privadas. Puesto que los perímetros de las redes inalámbricas no están bien definidos, se debe llevar a cabo una evaluación de riesgos en tales casos para identificar los controles (por ejemplo, autenticación fuerte, métodos criptográficos y selección de frecuencia) para mantener la separación de la red.

  Así mismo se debe tener en cuenta en la Segregación de redes, lo siguiente:

- La plataforma tecnológica critica de la ESDEG que soporta los sistemas de información debe estar separado en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a internet.
- La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos, de enrutamiento y de seguridad, si así se requiere DETIC, es la encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información trasmitida.

### 7.9.2 Política transferencia de información

7.9.2.1 Política procedimientos de transferencia e intercambio de información

Para el intercambio de información se debe tener en cuenta su grado de clasificación y los procedimientos establecidos que garanticen la integridad, confidencialidad y disponibilidad.

Se deben realizar procedimientos claros y controles para la utilización de servicios de comunicación electrónica en el intercambio de información, teniendo en cuenta los siguientes aspectos:

- Procedimientos para proteger la información a intercambiar contra interceptación, copiado, modificación, enrutamiento inadecuado y destrucción.
- Procedimientos para detección y protección contra códigos maliciosos que se pueden transmitir con el uso de comunicaciones electrónicas.
- Procedimientos para proteger la información electrónica sensible, que está en forma de archivo adjunto.
- Políticas o directrices que enfaticen el uso aceptable de los servicios de comunicación electrónica.

- Procedimientos para el uso de comunicaciones inalámbricas, pensando en los riesgos particulares involucrados.
- Establecer responsabilidades de funcionarios, contratistas y cualquier otro usuario que comprometan a la Institución, por ejemplo, a través de difamación, acoso, suplantación de identidad, envío de cartas de cadena, adquisición no autorizada, etc.
- Uso de técnicas criptográficas, para proteger la confidencialidad, la integridad y la autenticidad de la información.
- No dejar información sensible o crítica en los dispositivos de impresión como copiadoras, impresoras y máquinas de facsímil.
- Controles y restricciones con el envío de servicios de comunicación, como el envío automático de correo electrónico a direcciones de correo externas.
- Evitar dar información que pueda ser utilizada por personas externas al área de trabajo o a la institución con el fin de hacer ingeniería social.

7.9.2.2 Política acuerdos sobre transferencia de información

La ESDEG cumplirá lo estipulado en la Ley 594 de 2000, por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones, y que tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado.

7.9.2.3 Política mensajería electrónica (correo electrónico)

- La cuenta de correo electrónico institucional debe ser usada para el desempeño de las funciones asignadas dentro de cada una de las dependencias de la Entidad.
- Los mensajes y la información contenido en los buzones de correo institucional son de propiedad de la ESDEG; cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones; por ese motivo la información, y el tráfico de la misma, se considera de interés de sector.
- El tamaño de los buzones y mensajes de correo serán determinados por el DETIC, conforme a las necesidades de cada usuario y previa autorización del jefe inmediato.
- Toda información que requiera ser trasmitida fuera de la ESDEG, y que por sus características de confidencialidad e integridad debe ser protegida, debe estar en formatos no editables y con mecanismos de seguridad, solo puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.
- No se considera aceptado el uso de correo electrónico corporativo para los siguientes fines:

    - Enviar o trasmitir cadenas de correo, mensajes con contenidos religioso, político, racista, sexista, pornográfico, publicitario, no comparativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que pueden afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas promuevan actividad ilegal incluido el lavado de activos
    - El envío de cualquier tipo de archivo que ponga en riesgo la seguridad de la información; en caso de que sea necesario hacer un envío de este tipo de archivos deberá contar con la autorización correspondiente por parte de DETIC, o la que haga sus veces.
    - El envío de información relacionado con la defensa y la seguridad nacional a otras entidades de gobierno diferentes a las que conforman al sector defensa sin autorización previa del propietario de la información y de DETIC, o la que haga sus veces.

- Todo correo electrónico deberá respetar el estándar de formato e imagen institucional y deberá contener al final del mensaje un texto en español e inglés en el que se contemple, mínimo, los siguientes elementos:

    - El mensaje (incluyendo cualquier anexo) contiene información confidencial y se encuentra protegido por la ley.
    - El mensaje solo puede ser utilizado por la persona o empresa o la cual está dirigido.

- En caso de que el mensaje sea recibió por alguna personas o empresa no autorizada, solicita borrarlo de forma inmediata.
- Prohibir la retención, difusión, distribución, copia o cualquier otra acción basada en el mensaje.

7.9.2.4 Política acuerdos de confidencialidad o de no divulgación

Se deben establecer acuerdo de Confidencialidad o NDA (por las siglas en inglés de Non-Disclosure Agreement) con el objetivo de comprometer legalmente a las partes signatarias, a no revelar información que se divulga o intercambia entre la ESDEG y otras entidades para un objetivo o fin determinado, pero que no está o no debe alcanzar el domino público, y de ahí que deba guardarse confidencialmente. Debe incluir:

- Definir la información que se va a proteger (información confidencial).
- Determinar la duración esperada de un acuerdo, incluidos los casos en los que podría ser necesario mantener la confidencialidad indefinidamente.
- Establecer las acciones requeridas cuando termina el acuerdo.
- Definir las responsabilidades y acciones de los firmantes para evitar la divulgación no autorizada de información.
- Definir la propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de información confidencial.
- Definir el uso permitido de información confidencial y los derechos del firmante para usar la información.
- Establecer el derecho a actividades de auditoría y de seguimiento que involucran información confidencial.
- Definir el proceso de notificación y reporte de divulgación no autorizada o fuga de información confidencial.
- Definir los plazos para que la información sea devuelta o destruida al finalizar el acuerdo.
- Establecer las acciones que se espera tomar en caso de violación del acuerdo.

## 7.10 **POLITICAS DE ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**

El DETIC, velara que los sistemas de información que sean implementados en la entidad cumplan con los requerimientos de seguridad y buenas prácticas.

Todos los procesos de la entidad que realicen desarrollos deberán cumplir con los procedimiento y metodologías de desarrollo establecidos y formalizados para poder liberar sus aplicaciones.

Todos los procesos de la entidad deberán informar al área de tecnología sobre sus proyectos de adquisición de sistemas de información, con el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesario para su desarrollo e implementación.

### **7.10.1 Política requisitos de seguridad de los sistemas de información**

Se debe garantizar que la seguridad es una parte integral de los sistemas de Información, dentro de los cuales se incluyen sistemas operativos, infraestructura, aplicaciones servicios y aplicaciones desarrolladas para usuarios. El diseño y la implementación del sistema de información que da soporte a los procesos de las ESDEG que pueden ser críticos para la seguridad.

Se deben identificar y acordar los requisitos de seguridad antes del desarrollo y / o la implementación de los sistemas de información.

Todos los requisitos de seguridad se deben identificar en la fase inicial de un proyecto y se deben justificar, acordar y documentar como parte de todo el proyecto para un sistema de información.

7.10.1.1 Política análisis y especificación de requisitos de seguridad de la información

- Se deben declarar los requisitos para nuevos sistemas de información, mejoras a los sistemas existentes especificando los requisitos para los controles de seguridad.

- Se debe considerar los controles automatizados que se han de incorporar en el sistema de información y la necesidad de controles manuales de soporte; de igual manera aplica cuando se evalúan los paquetes de software, desarrollados o adquiridos, los requisitos de seguridad y los controles deben reflejar el valor de los activos de información involucrados y el daño potencial que se puede presentar debido a una falla o a la ausencia de seguridad.
- Los requisitos del sistema para la seguridad de los activos y la información y los procesos para Implementarla se deben documentar e integrar en las fases iniciales de los proyectos del sistema de información y deben ser objeto de pruebas de aceptación.
- Los contratos con el proveedor deberán abordar los requisitos de seguridad identificados.
- Cuando la funcionalidad de la seguridad de un producto determinado no satisface el requisito específico, entonces se debe considerar la inclusión de los controles a los riesgos, introducidos y asociados, antes de adquirir el producto.
- Cuando los productos requeridos proporcionan una funcionalidad adicional y ello causa un riesgo de seguridad, tal funcionalidad se debe inhabilitar o se deberá revisar la estructura del control propuesto para determinar si se puede obtener ventaja de la funcionalidad mejorada disponible.

7.10.1.2 Política seguridad de servicios de las aplicaciones en redes públicas

- Se deben evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.
- Se deben diseñar controles apropiados en las aplicaciones, incluyendo las aplicaciones desarrolladas por el usuario para garantizar el procesamiento correcto, estos controles deben incluir la validación de los datos de entrada, del procesamiento interno y de los datos de salida.
- Se pueden necesitar controles adicionales para los sistemas que procesan o tienen impacto en la información sensible, de valor o crítica. Dichos controles se deberían determinar con base en los requisitos de seguridad y en la evaluación de riesgos.

Validación de los datos de entrada

- Se deben realizar verificaciones de las entradas de las transacciones de los datos permanentes o requeridos (por ejemplo, nombres y direcciones).
- Se deben verificar las entradas duales u otras entradas, tales como verificación de fronteras o campos limitantes para especificar los rangos de los datos de entrada, con el fin de detectar los siguientes errores: valores fuera de rango, caracteres no válidos en los campos de datos, datos incompletos o ausentes, exceso en los límites superiores e inferiores del volumen de datos, datos de control inconsistentes o no autorizados.
- Se deben hacer revisiones periódicas del contenido de los campos clave o de los archivos de datos para confirmar su validez e integridad.
- Se deben inspeccionar los documentos de entrada impresos para determinar cambios no autorizados (todos los cambios en los datos de entrada deben estar autorizados).
- Se deben diseñar y documentar los procedimientos de respuesta ante errores de validación y procedimientos para probar la credibilidad de los datos de entrada.
- Se deben definir las responsabilidades para todo el personal que participa en el proceso de entrada de datos y se debe crear un registro de las actividades implicadas en el proceso de entrada de datos.
- Se debe pensar en la validación y el examen automático de los datos de entrada, cuando se puedan aplicar, para reducir el riesgo de errores y evitar ataques normales, incluyendo desbordamiento de búfer o inyección de códigos.

Control del procesamiento interno

- El diseño y la implementación de las aplicaciones debe garantizar que se minimizan los riesgos de falla en el procesamiento, que originan pérdida de la integridad y disponibilidad, para lo cual deben tener en cuenta como mínimo, procedimientos tales como: evitar que los programas se ejecuten en orden erróneo, utilización de programas para la recuperación después de fallas, protección contra

ataques empleando desbordamiento / exceso en el buffer, controles de sesión o de lotes, para conciliar los balances de archivos de datos después de actualizar las transacciones, controles para cada ejecución, totales de actualizaciones de archivos, controles programa a programa, validación de los datos de entrada generados por el sistema, verificaciones de la integridad, la autenticidad o cualquier otra característica de seguridad de los datos o del software descargado o actualizado entre el computador central y el remoto, totales de verificación (hash) de registros y archivos, verificaciones para garantizar que los programas de aplicación se ejecutan en el tiempo y orden correcto y terminan en caso de falla, deteniendo el procesamiento posterior hasta que se resuelve el problema, creación de un registro de las actividades implicadas en el procesamiento.

- Los datos que se han ingresado correctamente se pueden corromper por errores de software, de procesamiento o a través de actos deliberados, por tal razón se deben realizar verificaciones de validación que dependen de la naturaleza de la aplicación y del impacto de la corrupción de los datos en la organización.

Autenticación de los mensajes

- Se deben identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.
- Se deben realizar una evaluación de los riesgos de seguridad para determinar si se requiere integridad del mensaje y para identificar el método más apropiado de Implementación, haciendo uso de técnicas criptográficas como un medio de autenticación del mensaje.

Validación de los datos de salida

Comúnmente, los sistemas y las aplicaciones se construyen asumiendo que al realizar la validación, la verificación y las pruebas adecuadas, la salida siempre será correcta. Sin embargo, esta suposición no siempre es válida; es decir, los sistemas que se han sometido a prueba aún pueden producir salidas incorrectas en algunas circunstancias.

- Se deben validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias.
- La validación de los datos de salida puede incluir:
  - Verificaciones de la calidad y razonabilidad de los datos de salida.
  - Suministro de información suficiente para que un lector o un sistema de procesamiento posterior determine la exactitud, totalidad, precisión y clasificación de la información.
  - Procedimientos para responder las pruebas de validación de salidas.
  - Definición de las responsabilidades de todo el personal que participa en el proceso de la salida de datos.
  - Creación de un registro de las actividades del proceso de validación de la salida de datos.

7.10.1.3 Política protección de transacciones de los servicios de las aplicaciones

Se deben implementar Módulos de Seguridad de Hardware que proporcionen protección para las transacciones, identidades y aplicaciones, asegurando claves criptográficas y el aprovisionamiento de cifrado, descifrado, autenticación y servicios de firma digital para las aplicaciones, así:

- Definir el uso de firmas electrónicas por cada una de las partes involucradas en la transacción.
- Definir la trayectoria de las comunicaciones entre todas las partes involucradas esté encriptada.
- Definir los protocolos usados para comunicarse entre todas las partes involucradas estén asegurados.
- Asegurar que el almacenamiento de los detalles de la transacción esté afuera de cualquier entorno accesible públicamente, (en una plataforma de almacenamiento existente en la intranet de la organización, y no retenido ni expuesto en un medio de almacenamiento accesible directamente desde Internet).
- Utilizar una autoridad confiable (para los propósitos de emitir y mantener firmas digitales o certificados digitales), la seguridad está integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro.

- Establecer todos los aspectos de la transacción, es decir, asegurar que:

  - Definir la información de autenticación secreta de usuario, de todas las partes, se valide y verifique.
  - Definir la transacción que permanezca confidencial.
  - Mantener la privacidad asociada con todas las partes involucradas.

### 7.10.2 Política seguridad en los procesos de desarrollo y de soporte

7.10.2.1 Política de desarrollo seguro

El desarrollo de software, las actualizaciones y las nuevas versiones únicamente se deben pasar a producción e implementación después de obtener la aceptación formal.

7.10.2.2 Política procedimientos de control de cambios en sistemas

- Los procedimientos formales de control de cambios deben ser documentados y solo entran en producción después de la aprobación por el dueño del aplicativo y cumplimiento del control de calidad.
- Los controles de cambio deben incluir una evaluación de riesgos, análisis de los impactos de los cambios y especificación de los controles de seguridad necesarios.
- Se debe dar acceso a los programadores de soporte sólo a aquellas partes del sistema necesarias para su trabajo y que existe un acuerdo y aprobación formal para cualquier cambio.
- Siempre que sea factible, en los procedimientos de control de cambios operativos y de aplicación se deben tener en cuenta los siguientes aspectos:

  - La verificación de los niveles acordados de autorización.
  - La garantía de que los cambios son realizados por personal autorizado y capacitado.
  - La revisión de los controles y de los procedimientos de integridad para asegurar que no se pondrán en peligro debido a los cambios.
  - La identificación de todo el software, la información, las entidades de bases de datos y del hardware que requieran mejora.
  - La obtención de la aprobación formal de las propuestas detalladas antes de iniciar el trabajo.
  - Actualizar la documentación del sistema al finalizar cada cambio.
  - Verificar que la documentación operativa y los procedimientos de usuario se cambian en función de la necesidad con el objeto de mantener su idoneidad.
  - Realizar la implementación de los cambios en el momento oportuno y verificar que no se perturban los procesos de los servicios involucrados.

7.10.2.3 Política revisión técnica de las aplicaciones después de cambios en la plataforma de operación

- Se deben revisar los procedimientos de integridad y control de la aplicación para asegurarse de que no se han puesto en peligro, debido a los cambios en el sistema operativo.
- Se debe incluir en el plan y el presupuesto de soporte anual las revisiones y pruebas del sistema que resulten de cambios en el sistema operativo.
- Se debe notificar oportunamente sobre los cambios en el sistema operativo para permitir la realización de las pruebas y las revisiones apropiadas antes de la implementación.
- Se deben monitorear las vulnerabilidades y las nuevas versiones de parches y arreglos (fixes) ofrecidos por el distribuidor.

7.10.2.4 Política restricciones en los cambios a los paquetes de software

- Se deben controlar todos los cambios o modificaciones a los paquetes de software, y limitarlos a los cambios necesarios.
- Se debe implementar un proceso de gestión de las actualizaciones del software para asegurarse de que los últimos parches aprobados y mejoras de las aplicaciones están instalados en todo el software

autorizado. Todos los cambios se deben probar y documentar en su totalidad de manera que se puedan volver a aplicar, si es necesario, para mejoras futuras del software.

- Los paquetes de software suministrados por terceras partes se deben usar sin modificaciones. Cuando sea necesario modificar un paquete de software, se deben tener en cuenta los siguientes puntos:

    - El riesgo de que los procesos de integridad y de control incorporados se vean comprometidos.
    - Si es necesario, obtener el consentimiento del vendedor.
    - La posibilidad de obtener los cambios requeridos del vendedor como un programa estándar de actualizaciones.
    - El impacto, si la Institución se hace responsable del mantenimiento futuro del software como resultado de los cambios. Si los cambios son necesarios, el software original se deberá conservar y los cambios se deben aplicar a una copia claramente identificada.

7.10.2.5 Política principios de construcción de sistemas seguros

- Seguir principios de la ingeniería del software:
    - Siempre se debe trabajar con privilegios mínimos.
    - Simplicidad en el diseño: KISS.
    - Diseño abierto: no hay que depender de la ocultación.
    - Mediación completa: todos los accesos se controlan.
    - Valores por defecto seguros: acceso cerrado.
    - Separación de privilegios: control acceso multi-nivel.
    - Mínimo uso de recursos compartidos (p.ej. /tmp).
    - Facilidad de uso: los usuarios colaboran más.

- Interfaz segura: debe ser mínima (simple), dar acceso a las funciones justas y no ser evitable. Siempre se asume que la confianza es mínima.
- Separación de control y datos: no se debe soportar el uso de macros almacenadas en los documentos.
- Minimización de privilegios: Concesión de privilegios mínimos, se abandonan en cuanto no son necesarios (ej. apertura puertos TCP), se controla su tiempo de validez y se conceden al mínimo número de módulos posible.
- Valores por defecto seguros:
    - Instalación por defecto con muchas restricciones, el usuario es el que las relaja si es necesario.
    - Nunca se instala nada con claves por defecto,
    - Los programas se deben instalar de manera que no sean modificables por los usuarios (permisos).
- Carga de valores iniciales segura: desde /etc./.
- Fallo seguro: Se cancela el proceso de una petición si hay errores de proceso de la entrada o inesperados.
- Evitar condiciones de carrera: Se producen cuando varios procesos se interfieren unos a otros; se pueden producir entre procesos en los que no confiamos (problemas de secuencia) o entre procesos en los que si confiamos (interbloqueo).
- Problemas de secuencia: se dan cuando se pueden producir cambios entre dos operaciones (la secuencia no es atómica); comunes al acceder a sistemas de archivos, sobre todo si se usan directorios compartidos (/tmp/).
- Interbloqueos: se pueden evitar reservando los recursos siempre en el mismo orden (desde todos los procesos).
- Confiar sólo en canales fiables: las direcciones origen IP o de correo pueden ser falseadas, el DNS no es un sistema seguro.
- Prevenir contenido malicioso cruzado mediante filtrado, codificación y validación de los datos de entrada.
- Ataques semánticos (el usuario piensa que hace una cosa y en realidad está haciendo otra), como por ejemplo el uso de URLs erróneos: se minimiza su efecto educando al usuario y dándole pistas de donde está en cada caso (ej.: http://foo.org@ham.net).

7.10.2.6 Política ambiente de desarrollo seguro

Se tendrá en cuenta Common Criteria o CC (ISO/IEC 15408:2009): estándar internacional para identificar y definir requisitos de seguridad. Se suele emplear para redactar dos tipos de documentos:

- Perfil de protección (Protection Profile o PP): es un documento que define las propiedades de seguridad que se desea que tenga un producto; básicamente se trata de un listado de requisitos de seguridad.
- Objetivo de seguridad (Security Target o ST): es un documento que describe lo que hace un producto que es relevante desde el punto de vista de la seguridad.
    - El primer paso para redactar un PP o un ST es identificar el entorno de seguridad: ¿En qué entorno vamos a trabajar? ¿Qué activos debemos proteger? ¿Para qué se va a usar el producto?
    - A partir de esta identificación obtenemos una serie de supuestos sobre el entorno (tipos de usuarios, tipo de red, etc.), una lista de posibles amenazas y una descripción de las políticas de seguridad de la organización.
    - Por último, se define un conjunto de objetivos de seguridad, demostrando que con ellos se combaten las amenazas y se cumplen las políticas.

7.10.2.7 Política desarrollo contratado externamente

- Acuerdos sobre licencias, propiedad de los códigos y derechos de propiedad intelectual.
- Certificación de la calidad y exactitud del trabajo realizado.
- Convenios de fideicomiso en caso de falla de la tercera parte.
- Derechos de acceso para auditar la calidad y exactitud del trabajo realizado.
- Requisitos contractuales para la calidad y la funcionalidad de la seguridad del código.
- Realización de pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

7.10.2.8 Política pruebas de seguridad de sistemas

- Auditoría de Seguridad: permitir el registro de eventos (hay que identificar cuáles pueden ser interesantes desde el punto de vista de la seguridad).
- No rechazo (Non-repudiation): uso de técnicas para verificar la identidad del emisor y/o el receptor de un mensaje.
- Soporte criptográfico: si se usa criptografía ¿qué operaciones la usan? ¿qué algoritmos y tamaños de clave se utilizan? ¿cómo se gestionan las claves?
- Protección de datos de usuario: especificar una política para la gestión de datos de usuario (control de acceso y reglas de flujo de información).
- Identificación y autenticación: uso de técnicas de validación de identidad.
- Gestión de seguridad: definición de perfiles de usuario y niveles de acceso asociados.
- Privacidad: soporte del anonimato de los usuarios.
- Autodefensa: la aplicación debe incluir sistemas de validación de su funcionamiento y fallar de manera segura si esa validación no se cumple.
- Utilización de recursos: soporte a la asignación de recursos, tolerancia a fallos, ...
- Control de acceso: soporte de sistemas que limiten el número y tipo de sesiones, el nivel de concurrencia y que proporcionen información sobre sesiones anteriores al usuario para ayudar a la detección de intrusos.
- Rutas o canales fiables: existencia de mecanismos que permitan al usuario identificar que accede a la aplicación real (p. ej. certificados digitales) evitando ataques del tipo hombre en el medio.

7.10.2.9 Política prueba de aceptación de sistemas

- Evidencia de que se ha tenido en cuenta el efecto del sistema nuevo en toda la seguridad de la Institución.
- Establecimiento de controles de seguridad.
- Requisitos de desempeño y capacidad de los computadores.
- Procedimientos de recuperación por errores, reinicio y planes de contingencia.
- Preparación y prueba de procedimientos operativos de rutina para las normas definidas.

- Procedimientos y manuales eficaces.
- Disposiciones para la continuidad operativa de la Institución.
- Evidencia de que la instalación del sistema nuevo no afectará adversamente a los sistemas existentes, particularmente en los momentos pico de procesamiento, como el final de mes.
- Transferencia tecnológica en el funcionamiento o utilización de los sistemas nuevos.
- Facilidad de uso, en la medida en que afecte el desempeño del usuario y evite el error humano.

### 7.10.3 Política datos de prueba

7.10.3.1 Política protección de datos de prueba

Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.

- Estableciendo los procedimientos de control de acceso, que se aplican a los sistemas de aplicación operacionales; se debe aplicar también a los sistemas de aplicación de pruebas;
- Teniendo una autorización separada cada vez que se copia información operacional a un ambiente de pruebas.
- Definiendo que la información operacional se debe borrar del ambiente de pruebas inmediatamente después de finalizar las prueba.
- Estableciendo que el copiado y uso de la información operacional se debe registrar en bitácoras (logs) para suministrar un rastro de auditoría.

## 7.11 POLITICAS RELACIONES CON LOS PROVEEDORES

La ESDEG establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación que tenga relación con la seguridad de la información.

Antes de Iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesario durante y después del contrato.

Se deben establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la ESDEG.

Se deben establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información de la ESDEG, las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.

Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas a la ESDEG. El resultado del análisis de riesgos será la base para el establecimiento de los controles en la matriz de riesgo, que se definirá en el proyecto de pliegos del contrato.

Los funcionarios de la ESDEG, que ejercen como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.

En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información.

Los proveedores y/o contratistas solo podrán tener acceso a los activos de información necesarios para el desarrollo de sus obligaciones contractuales.

El acceso de proveedores y/o contratistas a los sistemas de información estará definido por usuario y contraseña el cual tendrá el nivel de acceso requerido para el desarrollo de sus obligaciones contractuales.

Los proveedores y/o contratistas al dejar de prestar sus servicios a la ESDEG, deben entregar toda información del producto del trabajo realizado y hacer entrega de los equipos y recursos tecnológicos en perfecto estado, de acuerdo con las condiciones establecidas en el contrato o convenio. Una vez terminada la relación contractual, debe comprometerse a no utilizar, comercializar o divulgar la información generada o conocida durante la gestión en la ESDEG, directamente o a través de terceros.

### 7.12 POLITICAS GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los alumnos, personal de planta, prestadores de servicios, contratistas o terceras partes deberán informar o reportar inmediatamente al DETIC por cualquiera de los medios dispuestos para tal fin, cada vez que detecten cualquier situación sospechosa, evento, incidente o debilidad que comprometa la seguridad de la información.

Sera responsabilidad del DETIC seguir los procedimientos establecidos para la gestión de los incidentes que puedan presentarse.

En el procedimiento se indica como responde la entidad en caso de presentarse algún incidente que afecte alguno de los 3 servicios fundamentales de la información: Disponibilidad, Integridad o confidencialidad. Se debe especificar:

- Los roles, las responsabilidades y acciones requeridas para identificar, contener, documentar, recolectar evidencias.
- Requisitos para mejorar la respuesta ante un incidente de seguridad de la información.
- indicar en qué casos sería necesario pasar a la activación de los planes de BCP (Planes de Continuidad) dependiendo de la criticidad de la información.
- Reporte de debilidades de seguridad de la información.
- Evaluación de eventos de seguridad de la información y decisiones sobre ellos.
- Aprendizaje obtenido de los incidentes de seguridad de la información.

El incidente informático debe ser reportado por el usuario al Oficial de Seguridad de la Información, quien lo evaluará e informará al Comando Conjunto Cibernético y este a su vez al grupo de respuesta a incidentes de seguridad de cómputo (CSIRT) de ser necesario.

La ESDED cuenta con el Procedimiento gestión de incidentes de seguridad de la información y el formato bitácora incidentes de seguridad de la información.

### 7.13 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

La ESDEG establecerá un plan de continuidad tecnológica donde se debe incluir la continuidad de la seguridad de la información y restauración oportuna de los servicios en un escenario de contingencia.

El DETIC generará dicho plan de continuidad tecnológica con base a Planes de Recuperación de Desastres (DRP) y Análisis de Impacto al Negocio (BIA).

#### 7.13.1 Política continuidad de la seguridad de la información

Se deben Identificar y documentar los eventos (o secuencia de eventos) que pueden causar interrupciones en los procesos de la organización, por ejemplo, fallas de los equipos, errores humanos, robo, desastres naturales y actos terroristas.

Se deberá continuar con una evaluación de riesgos para determinar la probabilidad y el impacto de tales interrupciones, en términos de tiempo, escala de daño y periodo de recuperación.

Se debe hacer una evaluación donde se identifique, cuantifique y prioricé los riesgos frente a los criterios y los objetivos pertinentes para la Institución, incluyendo los recursos críticos, impactos de las interrupciones, duración permitida de corte y prioridades de recuperación.

Se debe desarrollar una estrategia de continuidad de los servicios informáticos para determinar el enfoque global. Una vez se ha creado esta estrategia, el jefe de DETIC debe aprobarla y crear y respaldar un plan de contingencia para la implementación de esta estrategia.

7.13.1.1 Política planificación de la continuidad de la seguridad de la información

- Identificar los requisitos de seguridad de la información.
- Identificar las condiciones para la activación de los planes que describan el proceso a seguir (por ejemplo, la forma de evaluar la situación y quién se va a involucrar) antes de activar cada plan.
- Documentar los procedimientos de emergencia que describan las acciones a realizar tras un incidente que ponga en peligro las operaciones informáticas.
- Documentar los procedimientos de respaldo que describan las acciones a realizar para desplazar las actividades esenciales o los servicios de soporte a lugares temporales alternos y devolver la operatividad de los procesos informáticos en los plazos requeridos.
- Documentar los procedimientos operativos temporales a seguir mientras se terminan la recuperación y la restauración.
- Programar el mantenimiento que especifique cómo y cuándo se realizarán pruebas al plan y el proceso para el mantenimiento del mismo.
- Realizar actividades de concientización, educación y formación diseñadas para comprender los procesos de continuidad del negocio y garantizar que los procesos siguen siendo eficaces.
- Identificar y responsabilizar a las personas, encargadas de la ejecución de cada componente del plan; si se requiere se deberán nombrar los suplentes.
- Identificar los activos y recursos críticos necesarios para ejecutar los procedimientos de emergencia, respaldo y reanudación.

7.13.1.2 Política implementación de la continuidad de la seguridad de la información

- Se debe identificar, acordar y documentar todas las responsabilidades y los procedimientos para la continuidad de los servicios informáticos.
- Se deben implementar los procedimientos que permitan recuperar y restaurar los sistemas de información y la disponibilidad de los datos en las escalas de tiempo requeridas; es necesario atender la evaluación de las dependencias internas y externas y de los contratos establecidos.
- Se deben documentar los procedimientos y procesos acordados (manual de Funciones y Procedimientos).
- Se deben hacer pruebas periódicas y actualización de los planes de contingencia.

7.13.1.3 Política verificación, revisión y evaluación de la continuidad de la seguridad de la información.

- Se debe hacer una prueba sobre papel de varios escenarios, analizando las disposiciones de recuperación con ayuda de ejemplos de interrupciones.
- Se deben realizar simulaciones, particularmente para la formación del personal en sus funciones de gestión de crisis / post-incidentes.

- Se deben realizar pruebas de recuperación técnica, garantizando que los sistemas de información se pueden restaurar eficazmente.
- Se deben realizar pruebas de los recursos y servicios del proveedor, asegurando que los servicios y productos proporcionados externamente cumplirán el compromiso contraído.
- Se deben realizar ensayos completos del plan, probando que la organización, el personal, el equipo, las instalaciones y los procesos puedan hacer frente a las interrupciones.

### 7.13.2 Política redundancias

Procurar que el respaldo de la información sea redundante, es decir; que la información sea respaldada en dos medios diferentes y que una de estas copias permanezca en un lugar aparte y seguro del sistema.

7.13.2.1 Política disponibilidad de instalaciones de procesamiento de información

- La responsabilidad de la continuidad se delega en el DETIC, para lo cual se debe elaborar el plan formal de continuidad de negocio y recuperación de desastres, que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales.
- En el plan de continuidad se deben definir las necesidades de elementos redundantes.

## 7.14 POLITICAS DE CUMPLIMIENTO

La ESDEG velará por el cumplimiento de la legislación vigente respecto a los requisitos establecidos en la seguridad y privacidad de la información, derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública.

En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, la ESDEG tomará las acciones disciplinarias y legales correspondientes.

### 7.14.1 Política de cumplimiento de requisitos legales y contractuales

7.14.1.1 Política identificación de la legislación aplicable y de los requisitos contractuales.

La ESDEG tendrá en cuenta la legislación aplicable garantizando su ordenamiento, actualización y consulta mediante normograma de cada proceso.

7.14.1.2 Política derechos de propiedad intelectual.

- La ESDEG cumplirá con la reglamentación vigente sobre propiedad intelectual, para lo cual implementarán los controles necesarios que garanticen el cumplimiento de dicha reglamentación.
- No se permitirá el almacenamiento, descarga de internet, intercambio, uso copia, reproducción y/o instalación de software no autorizado, música, videos, textos, fotografías y demás obras protegidas por derecho de propiedad intelectual será de quien lo desarrolle que no cuenten con la debida licencia o autorización legal.
- Se permitirá el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de los mismos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.

- Los procesos de adquisición de aplicaciones y paquetes de software cumplirán con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derecho de autor y con los procedimientos establecidos por el Ministerio de Defensa Nacional y el Comando General de las Fuerzas Militares.
- El software a la medida, adquirido a terceras partes o desarrollado por funcionarios de la institución o entidades del sector defensa, será de uso exclusivo de dicha entidad y la propiedad intelectual será de quien lo desarrolle.
- La adquisición de aplicaciones y paquetes de software, así como el desarrollo de software a la medida deberá contar con la aprobación DETIC y/o por quien determine el Ministerio de Defensa Nacional y el Comando General de las Fuerzas Militares.

7.14.1.3 Política protección de registros.

Es necesario determinar los niveles de protección de los registros para así evitar cambios en la información que contienen, por ejemplo, protección con contraseña o existencia de archivos con acceso restringido.

Un aspecto fundamental es la realización de copias de seguridad de los registros digitales de la entidad.

7.14.1.4 Política privacidad y protección de información de datos personales

Asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable. Para dar cumplimiento, la ESDEG cuenta con el procedimiento de Tratamiento y protección de Datos personales y el Formato autorización de tratamiento y protección de datos personales.

Datos 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.

Se prohíbe el Tratamiento de datos sensibles, excepto cuando:

- El Titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
- El tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado; en estos eventos, los representantes legales deberán otorgar su autorización.
- El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad; en estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.
- El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- El Tratamiento tenga una finalidad histórica, estadística o científica; en este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

El titular de los datos personales tendrá los siguientes derechos:

- Conocer, actualizar y rectificar sus datos personales en su calidad de responsable del tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o a aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Solicitar prueba de la autorización otorgada a la ESDEG salvo cuando expresamente se exceptúe como requisito para el tratamiento con lo previsto en el artículo 10 de la Ley 1581 de 2012.
- Ser informado por la ESDEG, previa solicitud, respecto del uso que les ha dado a sus datos personales.
- Solicitar prueba de la autorización otorgada al responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento.
- Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a la Ley 1581 de 2012 y a la Constitución.
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

Deberes de la ESDEG

- Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Solicitar y conservar, copia de la respectiva autorización otorgada por el Titular.
- Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- Actualizar la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.
- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.
- Suministrar al encargado del tratamiento de los datos, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado por el titular.
- Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
- Tramitar las consultas y reclamos formulados por el titular de la información.
- Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento, para la atención de consultas y reclamos.
- Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
- Informar a solicitud del Titular sobre el uso dado a sus datos.
- Dar cumplimiento al principio de seguridad establecido en la normatividad vigente, la ESDEG adoptará las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio, el Ministerio de Tecnologías de la Información y las Comunicaciones y/o el Ministerio de Defensa Nacional.

Modificaciones a las condiciones de uso

- La ESDEG podrá modificar las Políticas de Privacidad aquí contenidos, a su libre elección y en cualquier momento y los mismos estarán vigentes una vez hayan publicado en la página web.

- El usuario se compromete a revisar periódicamente esta sección para estar informado de tales modificaciones y cada nuevo acceso del usuario a la página será considerado una aceptación tácita de las nuevas condiciones.
- El tratamiento de los datos personales por parte de la ESDEG requiere de la autorización previa, libre, expresa e informada por parte del titular.

Autorización del titular y suministro de información

El tratamiento de los datos personales por parte de la ESDEG requiere de la autorización previa, libre, expresa e informada por parte del titular.

Para el suministro de la información solicitada por el Titular, podrá ser suministrada por cualquier medio ya sea documento físico, de forma oral, electrónica (mensaje de datos, internet, sitios web) o cualquier medio que evidencien el otorgamiento de dicha información donde se incluirá autorización expresa por parte del titular de la información.

La autorización del titular no será necesaria cuando se trate de:

- Información requerida por una Entidad Pública o Administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Datos de urgencia médica o sanitaria.
- Tratamiento de Información autorizado por la Ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

A quienes se les puede suministrar la información:

- Al titular quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición la ESDEG.
- Por los causa habientes del titular quienes deberán acreditar tal calidad.
- Por el representante y/o apoderado del titular previa acreditación de la representación o poder respectivo.
- A los terceros autorizados por el titular o por la ley, previa acreditación de autorización escrita y autenticada.

Procedimiento para consultas, reclamos, actualización y rectificación

- Los titulares podrán CONSULTAR la información personal del titular que repose en la ESDEG, por lo tanto, dicha consulta se deberá formular a través del correo electrónico pqrs@esdegue.edul.co.

- La consulta se resolverá en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo; de no ser posible su atención en este término se informará al solicitante el motivo de la demora y se señalará la fecha en que se resolverá la consulta la cual no podrá superar los 5 días hábiles subsiguientes al vencimiento del primer término.

- RECLAMOS: El titular que considere que la información contenida en una base de datos debe ser objeto de corrección, actualización y supresión o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley; podrán presentar un reclamo a través del correo electrónico pqrs@esdegue.edu.co

  El reclamo se formulará mediante solicitud escrita a través del correo electrónico dirigido a la ESDEG; con la identificación del titular, la descripción de los hechos que dan lugar al reclamo, la dirección y

acompañamiento de los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas.

Transcurridos dos (2) meses desde la fecha del requerimiento sin que el solicitante presente la documentación requerida se entenderá que ha desistido del reclamo.

Una vez recibido el reclamo completo, a través del correo establecido, este se nominará como "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha nominación deberá mantenerse hasta que el reclamo sea decidido.

El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

- La ESDEG tiene la obligación de validar, rectificar y actualizar a solicitud del titular la información que resulte ser incompleta o inexacta de conformidad con el procedimiento y los términos señalados para lo cual, el titular del derecho allegará la solicitud al correo electrónico pqrs@esdegue.mil.co informando de la actualización, rectificación y/o supresión del dato que se ha de modificar, aportando la documentación que soporte su solicitud.

- Los titulares de los datos personales pueden revocar el consentimiento al tratamiento de sus datos personales en cualquier momento, siempre y cuando no lo impida una disposición legal o contractual. Para ello la ESDEG dispone para uso del titular el email pqrs@esdegue.edu.co

### 7.14.2 Política revisiones de seguridad de la información

El Comité de Seguridad y privacidad de la información debe poner en marcha la revisión independiente y la realización de pruebas de vulnerabilidad en sus dependencias, con personal idóneo y capacitado en el área de Seguridad de la Información que debe ser solicitado a DETIC.

Esta revisión independiente es necesaria para asegurar la eficacia, idoneidad y propiedad del enfoque de la Institución para la gestión de la seguridad de la información. La revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluyendo la política y los objetivos de control.

Dicha revisión debe ser realizada por personas independientes del área sometida a revisión, por ejemplo, la auditoría interna, el Oficial de Seguridad de la Información de otra unidad y / o una organización externa especializada en tales revisiones.

Los resultados de la revisión independiente se deben registrar y reportar a la Unidad que ha iniciado la revisión. Estos registros se deben conservar.

Si la revisión identifica que el enfoque y la implementación de la seguridad de la información son inadecuados o no cumplen la orientación para la seguridad de la información establecida en el documento de políticas de la seguridad de la información, se deben considerar las acciones correctivas.

7.14.2.1 Política revisión independiente de la seguridad de la información

De ser necesario, se debe contratar asesoría externa especializada en el área de Seguridad de la Información para controlar y proteger los activos informáticos de la Institución. Así como para capacitar y entrenar y certificar al personal involucrado en el área de gestión de Seguridad de la Información.

7.14.2.2 Política cumplimiento con las políticas y normas de seguridad.

La oficina de planeación y el SGI-ESDEG se encargarán de:

- Controlar el cumplimiento y ejecución de las actividades programadas en la presente Directiva.
- Evaluar si la presente Directiva cumplió con el propósito para el cual fue diseñada y presenta recomendaciones para que su desarrollo sea eficaz.
- Establecer los mecanismos necesarios para el cabal cumplimiento del cronograma de trabajo establecido.

7.14.2.3 Política revisión de cumplimiento técnico.

El DETIC realizará evaluaciones de seguridad técnicas por o bajo la supervisión de personal de seguridad de la información o externo autorizado, apoyado en herramientas automáticas o con revisiones manuales realizadas por especialistas.

Mencionadas revisiones deben ser programadas y registradas como evidencia y a sus resultados se les hará seguimiento para asegurar que las brechas de seguridad fueron solucionadas.

**CONTROLDE CAMBIOS**

| No. Versión | Fecha Versión | Descripción del Cambio |
|---|---|---|
| 1 | 31-MAY-2022 | Elaboración Manual Políticas de seguridad y privacidad de la información |
| 2 | 30-MAR-2023 | Revisión y actualización del Documento. |

| LABORÓ: | APROBÓ: |
|---|---|
| Profesional de Defensa BLANCA SANTANA RODRIGUEZ<br>Ingeniera de Sistemas<br>Departamento TIC – ESDEG – COGFM | Capitán de Corbeta VELASCO GAITAN MANUEL ANTONIO<br>Jefe Departamento TIC- ESDEG |