1.PROCESO: TIC									
2.TIPO DE PROCESO	**Estratégico**		**Misional**		**Apoyo**	**x**	**Seguimiento y evaluación**		
3. OBJETIVO	Establecer y divulgar las Politicas de Seguridad y Privacidad de la Información de la Dirección de Veteranos y Rehabilitación Inclusiva del DIVRI de Defensa Nacional - DIVRI a funcionarios, pasantes y contratistas, proveedores incluyendo personal suministrado por terceros que provean servicios a la DIVRI, entidades públicas y privadas y demás partes interesadas, esto con el fin de darlas a conocer para su respectivo cumplimiento.								
4.RESPONSABLE	Líder Proceso TIC								
5. ALCANCE	Las políticas de seguridad y privacidad de la información son aplicables para todos los aspectos administrativos, técnicos, tecnológicos y de control que deben ser cumplidas por directivos, funcionarios, contratistas, pasantes, proveedores, entidades públicas y privadas, ciudadanos y demás partes interesadas, que cumplan con alguna de las siguientes condiciones: a. Acceso a la información tanto física como lógica. b. Ingreso de manera física a las instalaciones o lógica a través de la plataforma tecnológica de la DIVRI. c. Uso de equipos informáticos y de telecomunicaciones conectados a la plataforma tecnológica. d. Uso de los servicios informáticos dispuestos por la DIVRI a través de los canales digitales. e. Diseño, construcción, pruebas, implementación o uso de herramientas tecnológicas o servicios informáticos dispuestos por la DIVRI para el desarrollo de sus funciones. Se adoptan los términos y definiciones de la familia de normas técnica ISO 27000 vigentes, y de los estándares que se apliquen de acuerdo con el alcance de las políticas. **Activo:** cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. **Activo de Información:** recurso o elemento que contiene información con valor para la organización debido a su utilización en algún proceso o que tiene relación directa o indirecta con las funciones de la entidad: software, hardware, personas (roles), físicos (instalaciones, áreas de almacenamiento de expedientes, centros de procesamiento de datos), intangibles								

	(imagen y reputación).
6. DEFINICIONES	**Amenaza:** causa potencial de un incidente no deseado que pueda provocar daños a un sistema o a la organización. **Amenaza informática:** situación potencial o actual que tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado **Antivirus:** programas cuyo objetivo es detectar y eliminar software malicioso. **Análisis de riesgos:** proceso para comprender la naturaleza del riesgo y determinar su nivel de riesgo. **Ataque:** Tentativa de destruir, exponer, alterar, inhabilitar, robar o acceder sin autorización o hacer un uso no autorizado de un activo. **Atributo:** Propiedad o característica de un objeto que puede ser cuantitativa o cualitativamente distinguible por medios humanos o automáticos. **Anonimización del dato:** eliminar o sustituir algunos nombres de personas (físicas o jurídicas), direcciones, información de contacto, números identificativos, apodos o cargo por otros datos para evitar la identificación de personas y preservar la confidencialidad de la información. **Archivos PST:** son archivos electrónicos creados desde el software de mensajería Outlook con el fin de almacenar de forma local (computadores), copia de elementos de un buzón de correo electrónico **Autenticación:** mecanismo técnico que permite garantizar que una persona o entidad es la correcta. **Autenticidad:** Propiedad de que una entidad es lo que afirma ser. **Back up:** se refiere a una copia de respaldo de información. **Buzón:** espacio de almacenamiento de información reservado en un servidor de correo electrónico con fines de almacenar correos, contactos, calendario, entre otros. Canal de comunicación: medio utilizado para la transmisión de información, por ejemplo: el cableado, fibra óptica y la atmósfera. **Centro de cómputo:** espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización llamado también data center por su término anglosajón. **Ciberseguridad:** capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. **Ciberespacio:** ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. **Confiabilidad:** persona o cosa en la que se puede confiar. **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. **Control de acceso:** Se adoptan los términos y definiciones de la familia de normas técnica ISO 27000 vigentes, y de los estándares que se apliquen de acuerdo con el alcance de las políticas. **Control informático:** las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas

para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo reduciendo la probabilidad o impacto del evento.

Correo electrónico: servicio de red que permite a los usuarios enviar y recibir mensajes (también denominados mensajes electrónicos o cartas digitales) mediante redes de comunicación electrónica.

Claves, contraseña o password: forma de autentificación que utiliza información secreta o confidencial para controlar el acceso hacia algún recurso.

Criterios para adquisición de tecnología: condiciones o requisitos mínimos para tener en cuenta al momento de implementar y/o adquirir tecnología, como: Compatibilidad: el sistema a adquirir debe ser compatible con la tecnología e infraestructura que tiene la entidad. Calidad: se deben definir requisitos con los que se pueda evaluar la calidad, tales como reconocimiento de marca y tiempo en el mercado. Garantía: se deben tener en cuenta los plazos de vigencia de la garantía ofrecidos y los requeridos para el proceso de implementación, adaptación, pruebas, y puesta en funcionamiento. Acuerdos de servicio: se deben generar reglas para la prestación de los servicios para las diferentes tareas que surjan en las diferentes etapas para definir los tiempos de respuesta entre las dos partes. Mantenimiento, actualizaciones y soporte: se deben definir los tiempos o momentos para aplicar el mantenimiento, definir de qué manera se realizarán las actualizaciones, cada cuánto y cómo se realizarán. Además, se debe identificar el alcance del soporte que se realice. Transacciones: se deben identificar cuáles transacciones realiza el sistema, de qué manera las realiza y dónde se almacenan. Reportes o salidas: se deben identificar las salidas de información de los sistemas, reportes, consultas en pantalla o impresiones.

Custodio de activo de información: individuo, cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de cumplir y velar por el cumplimiento de los controles que el responsable del activo de información haya definido, con base en los controles de seguridad disponibles en la entidad.

Datos abiertos: son datos primarios o sin procesar. Los cuales son puestos a disposición de cualquier ciudadano con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Datos biométricos: parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (ej. huella digital o voz).

Datos personales 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.

Dato privado: dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

	Dato público: dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas. **Dato semiprivado:** es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios. □ DAFP: Departamento Administrativo de la Función Pública **Disco duro:** disco de metal cubierto con una superficie de grabación ferro magnético que pueden ser grabados, borrados y regrabados como una cinta de audio. **Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. **DVD**: Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad. **Evento y/o incidente de seguridad de la información:** ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información. **Gestión de claves:** son controles que realizan mediante la gestión de claves criptográficas. **Gestión de incidentes de seguridad de la información:** proceso para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. **Gestión de riesgos:** actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, comprende la identificación, evaluación y el tratamiento de riesgos. **Grupos de Valor:** para Función Pública corresponden a las entidades del estado, servidores públicos y ciudadanos. **Habeas data:** derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos. **Infraestructura tecnológica:** elementos de hardware, software y comunicaciones que soportan la operación de los diferentes servicios de la entidad, entre los cuales se encuentran: equipos de trabajo, equipos portátiles, impresoras, escáner, videocámaras, wifi, sistemas operacionales, herramientas ofimáticas e internet entre otros. **Impacto:** el coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc. **Integridad:** la propiedad de salvaguardar la exactitud y completitud de la información.

	Internet: corresponde a una interconexión de diferentes redes de computadoras, permitiendo la creación de una red única de alcance mundial. **Intranet:** red informática que utiliza la tecnología del Protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización. **Inventario de activos:** lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del Sistema de gestión de seguridad de la información, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012) **No repudio:** servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2). **Titular de la información**: persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley. **Teletrabajo:** actividad laboral que se desarrolla afuera de las instalaciones de la entidad, las cuales emplean tecnologías de la información y de la comunicación para su desarrollo. **Trazabilidad**: cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. **Vulnerabilidad:** debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).
	La Política general de seguridad y privacidad de la información de la DIVRI establece el compromiso de la DIVRI de asegurar la salvaguarda de la información institucional, implementando los mecanismos y controles adecuados para garantizar su confidencialidad, integridad, disponibilidad y privacidad de la información, con el fin de mantener la continuidad de las operaciones del DIVRI. Los mecanismos y controles implementados responden al alcance de las políticas específicas y su aplicación a nivel institucional. **8.1 ORGANIZACIÓN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN** **8.1.1. Organización interna** El Decreto 1874 de 2021 Por el cual se modifica la estructura del Ministerio de Defensa Nacional, se crean nuevas dependencias, funciones y se dictan otras disposiciones. El Manual Especifico de Funciones y de Competencias Laborales determina los empleos que conforman la planta de personal, y establece las funciones esenciales, generales, específicas y comunes definidas para todos los empleos identificados, de acuerdo con el nivel jerárquico de decisión, así como la conformación de las áreas funcionales del DIVRI.

8. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Para efectos de la coordinación de las actividades relacionadas con la gestión de la seguridad y privacidad de la información, el Comité de Gestión y Desempeño de la Dirección de Veteranos y Rehabilitación Inclusiva es el encargado de asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información. En relación con la evaluación de controles institucionales el Subcomité Institucional de Coordinación del de Control Interno de la Dirección de Veteranos y Rehabilitación Inclusiva DIVRI es el encargado de monitorear los controles para el aseguramiento de la información. Los responsables de los procesos y Coordinadores de Grupos son responsables de los procesos estratégicos, misionales, de apoyo y seguimiento y evaluación y de la custodia de la información, el cumplimiento normativo sobre los datos y los registros documentales, la actualización de los activos de información, la gestión de los riesgos asociados a los activos de información y las acciones de tratamiento pertinente. El proceso estratégico TICS, es responsable del gobierno de las tecnologías de la información de la DIVRI, de la seguridad informática, seguridad y privacidad de la información, aseguramiento de la infraestructura tecnológica. El proceso de Apoyo Gestión Documental es responsable de la gestión documental institucional acorde con los lineamientos del Archivo General de la Nación. El proceso de Apoyo Gestión del Talento Humano y Gestión contractual es responsable de la adquisición del capital humano requerido por la DIVRI para apoyar la gestión de los procesos institucionales, la gestión tecnológica y la seguridad y privacidad de la información. **8.1.2. Separación de deberes** La separación de deberes define los roles, responsabilidades y niveles de autoridad en la interacción de la seguridad y privacidad de la información, en concordancia con el Manual específico de funciones y competencias laborales, sin perjuicio de lo anterior se establecen los siguientes lineamientos: • El personal que realiza labores funcionales sobre sistemas de información, sean críticos o no, de la DIVRI no pueden tener a su cargo labores de administración técnica sobre la plataforma tecnológica (sistemas operativos, bases de datos, programas de aplicación, software de comunicaciones, entre otros) que soporten los sistemas de información. • El personal técnico del Proceso Estratégico TICS no debe tener decisión sobre los datos que se procesan en los sistemas de información de la DIVRI.

• El personal contratista y proveedor de servicios de tecnologías de información y comunicación, solo tendrá acceso a la plataforma tecnológica de la DIVRI en el marco de su objeto contractual.

8.1.3. Contacto con las autoridades y con grupos de interés especial

El Equipo de Respuesta a Incidentes de seguridad y privacidad de la Información, debe mantener contacto con autoridades cibernéticas y grupos de interés especial, como son:

a. ColCERT - Grupo de Respuesta a Emergencias Cibernéticas de Colombia.
b. CSIRT PONAL - Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional. • CCOCI – Conjunto Comando Operativo Cibernético de las Fuerzas Militares de Colombia.
c. CSIRT Gobierno MinTIC - Equipo de respuesta frente a Incidencias de seguridad informática del DIVRI de Tecnologías de la Información y las Comunicaciones.
d. Grupo de Protección de Datos Personales de la Superintendencia de Industria y Comercio.
e. Partes interesadas internas.
f. Ministerio de Defensa Nacional.
f Demás entes u organismos nacionales o internacionales que tengan relación con la gestión de la seguridad y privacidad de la información, así como también contacto con asociaciones profesionales que permitan la constante actualización del conocimiento en riesgos, ataques y medidas de mitigación.

8.1.4. Seguridad de la información en la gestión de proyectos de tecnologías de la información (TI)

8.1.4.1. Gestión de proyectos de TI

Acorde con la metodología de gestión de proyectos de la DIVRI y los lineamientos de Arquitectura Empresarial, la gestión de TI realiza el procedimiento de Arquitectura Empresarial orientado a:

• Establecer la estrategia de Tecnologías de la Información.
• Articular la Estrategia Institucional con la gestión tecnológica.
• Contar con el Plan Estratégico de Tecnologías de la Información
• Evaluar los Proyectos Institucionales con alcance tecnológico.
• Incorporar los requisitos de seguridad y privacidad de la información.
• Evaluar los riesgos que puedan llegar a impactar la confidencialidad. privacidad, integridad y disponibilidad de la información de la DIVRI.

8.1.4.2. Salida o transporte de Información sensible o crítica

La salida o transporte de información sensible o crítica deberá estar plenamente justificada y contar con la suscripción de un "Acuerdo de Confidencialidad", que detalle el objeto de la salida de información, transporte y uso final.

8.1.5. Dispositivos móviles

8.1.5.1. De propiedad de la DIVRI

Para los dispositivos móviles tales como portátiles, tablets, celulares, entre otros, el DIVRI cuenta con:

• Controles físicos, para el uso de los dispositivos móviles por parte del personal de la DIVRI. Son de aplicación los lineamientos y directrices definidos en los siguientes documentos:

* Procedimiento Administración y control de bienes devolutivos y de consumo.
* Documento Guía para el manejo administrativo de los bienes de propiedad de la Nación MDN.

8.1.6. Trabajo en casa

El proceso Estratégico Tecnologías de la Información implementa los controles de seguridad informática necesarios para establecer la conexión remota con los servicios de TI de la DIVRI por parte de los funcionarios en modalidad de teletrabajo, de acuerdo con los lineamientos que sobre el tema adopte la DIVRI y coordinados con el proceso de Apoyo Gestión Talento Humano.

Responsabilidades del proceso Estratégico Tecnologías de la Información realizará:

• El alistamiento de los equipos asignados por el Grupo Administrativo y Financiero al Funcionario en la modalidad de trabajo en casa.
• La asignación de credenciales para el acceso a los sistemas de información requeridos por el funcionario.
• En caso de requerirse acceso a un servicio TI específico, se asignará una VPN.

El funcionario en la modalidad de trabajo en casa, debe:

• Hacer uso adecuado y exclusivo de los recursos tecnológicos asignados (computador, tablet, portátil u otros) para el cumplimiento de las funciones asignadas.
• Asegurarse de mantener la debida integridad, confidencialidad y disponibilidad de la información, así como de la privacidad de los datos personales objeto del desarrollo de sus funciones.
• Presentar los recursos tecnológicos asignados para los mantenimientos preventivos programados por el proceso estratégico Tecnologías de la Información.
• Reportar a través de la Mesa de Ayuda soporte_tics@divri.gov.co cualquier evento relacionado con la funcionalidad de los recursos tecnológicos asignados.
• Abstenerse de instalar software o programas ejecutables en los equipos asignados sin previa autorización del proceso estratégico Tecnologías de la Información, quien verificará la necesidad y las implicaciones de seguridad de su instalación

8.1.7. Trabajo con Acceso Remoto

Para la realización de trabajo con acceso remoto por parte de funcionarios o personal contratista o proveedor:

• Está disponible el acceso a los servicios de aplicación a través del sitio web institucional www.DIVRI.gov co – DIVRI – intranet, con acceso mediante autenticación ante la red y el servicio de aplicación con usuario y contraseña asignado por el proceso estratégico Tecnologías de la Información.
• Se debe informar al proceso estratégico Tecnologías de la Información sobre el requerimiento de acceso a los servicios de TI a través de VPN, previa autorización del Director de la Entidad.

8.2. SEGURIDAD DEL RECURSO HUMANO

En lo que corresponde a la gestión del personal de planta del DIVRI, al proceso de apoyo gestión de Talento Humano aplica los lineamientos normativos y regulatorios vigentes. En lo que respecta al personal contratista o proveedor el proceso de apoyo gestión contractual en coordinación con las áreas que tiene bajo su cargo la función de supervisión, aplica los lineamientos normativos y legales para la contratación del personal requerido de acuerdo con las necesidades institucionales.

El personal de la DIVRI sin importar su tipo de vinculación es responsable de la custodia y uso adecuado de los

activos asignados en los que se incluyen: equipos (computadores, portátiles, medios de almacenamiento), datos e información, acceso a aplicativos y software, entre otros. Para todos los efectos, el personal del DIVRI deberá acoger las disposiciones de seguridad y privacidad de la información en este Manual.

8.2.1. Responsabilidad del personal

Todos los funcionarios, pasantes, contratistas y proveedores, así como las partes interesadas autorizados por el DIVRI para acceder a la plataforma tecnológica y de comunicaciones, sistemas de información o aplicativos, hardware de red y software operativo, de programación, entre otros, son responsables del cumplimiento de las políticas, directrices, procedimientos, estándares y controles de seguridad informática y de la seguridad y privacidad de la información definidas por la DIVRI.

La información almacenada en los equipos de cómputo (servidores, computadores, portátiles, dispositivos móviles y demás dispositivos de procesamiento y almacenamiento) de la DIVRI es propiedad del DIVRI y cada usuario es responsable de proteger su confidencialidad, privacidad, integridad y disponibilidad

8.2.2. Procesos disciplinarios

En caso de incumplimiento en lo establecido en esta política por parte del personal de planta, se comunicará al área correspondiente para que esta proceda conforme a los lineamientos de la gestión disciplinaria del DIVRI. El incumplimiento de esta política por parte del personal contratista o proveedor, se convertirá en una causal para determinar la terminación del contrato o convenio, sin perjuicio de la iniciación de otro tipo de acciones a las que haya lugar.

8.2.3. Terminación o cambio del tipo de vinculación laboral

Todo personal del DIVRI al momento de su retiro de la DIVRI, cambio de cargo o de área es responsable de entregar al Jefe inmediato o Supervisor del contrato los activos de información que se originen en desarrollo de sus funciones o actividad contratada. El Proceso Gestión del Talento Humano informa a las áreas responsables de gestionar los activos de la DIVRI, sobre el retiro, cambio de cargo o de área de los funcionarios, a fin de:

a. Inhabilitar o inactivar, según sea el caso, los usuarios y contraseñas asignados para acceder a los servicios de TI de manera inmediata.
b. Inhabilitar o inactivar de manera temporal o permanente, según sea el caso, el carné de ingreso a las instalaciones físicas del DIVRI.

El Proceso Gestión de Contratación informa las áreas responsables de gestionar la suspensión, cesión o terminación del contrato, a fin de:

a. Inhabilitar o inactivar, según sea el caso, los usuarios y contraseñas asignados para acceder a los servicios de TI de manera inmediata.
b. Inhabilitar o inactivar de manera temporal o permanente, según sea el caso, el carné de ingreso físico a las instalaciones del DIVRI.

Los Jefes de área, partiendo de la Alta Dirección a través de los diferentes niveles jerárquicos, así como los supervisores de contratos, deberán:

a. Garantizar la retención de la información almacenada en los equipos (computador, portátil o tablet o en medios de almacenamiento externos) asignados al funcionarios, pasantes o contratistas, antes de su retiro formal de la DIVRI.
b. Garantizar la copia de seguridad de la información a cargo de funcionarios, pasantes o contratistas, en los medios de almacenamiento de la DIVRI durante y antes de la terminación del vínculo laboral con el DIVRI.
c. Garantizar la salvaguarda de la información física en condiciones de disponibilidad, integridad, privacidad y confiabilidad.

Los funcionarios y contratistas deben:

- Realizar la devolución de los activos de información atendiendo los lineamientos definidos en:

  a. Procedimiento Administración y Control de Bienes Devolutivos y de Consumo
  b. Documento Guía para el Manejo Administrativo de los Bienes de Propiedad de la Nación DIVRI.

- Realizar la entrega al Grupo Administrativo y Financiero del carné que lo acredita como funcionario, pasante

o contratista del DIVRI, para su disposición final.

8.3. GESTIÓN DE ACTIVOS DE INFORMACIÓN

Se aplican los lineamientos definidos en el procedimiento Generación Y Gestion Del Inventario De Activos De Información del DIVRI.

8.3.1. Inventario de activos de información

Todo el personal del DIVRI sin importar su tipo de vinculación, debe mantener actualizado el inventario de activos de Información, en particular cuando se presenten cambios significativos en:

- Los objetivos estratégicos, políticas, directrices, procesos (procedimientos, guías, formatos, controles y riesgos).
- La estructura organizacional.
- En la infraestructura de tecnologías de información y comunicación que afecten los procesos que soporta la DIVRI.
- Las normas, regulaciones o estándares relacionados con la gestión de los activos de información.
- Cambios en el entorno que afecten la ejecución de los procesos

Todos los activos de información identificados en el inventario de activos deben tener un propietario o responsable asociado.

8.3.2. Propiedad de los activos de información

Los propietarios de los activos de información en cualquiera de sus tipos y disposición física o digital son responsables de:

a. Identificar, clasificar y actualizar los activos relacionados con sus respectivos procesos, de acuerdo con las disposiciones del numeral 8.3.1 Inventario de activos de información.

b. Garantizar que se documenten los controles apropiados para guardar la confidencialidad, integridad, privacidad y disponibilidad de los activos de información y de sus sistemas de información.

8.3.3. Uso adecuado de los activos y recursos de información

Toda la información del DIVRI sin importar el tipo de soporte (físico o digital) debe ser procesada y almacenada de acuerdo con su nivel de clasificación, de manera que se protejan las propiedades de confidencialidad, privacidad, integridad y disponibilidad. El personal de la DIVRI independiente del tipo de vinculación, deberá cumplir los siguientes lineamientos:

a. No realizar cambios en la configuración del hardware o software de los equipos (computadores, portátiles o tablets) asignados o delegados para el desarrollo de sus funciones o del objeto contractual.
b. Solo las personas autorizadas por la Oficina de Sistemas de Información podrán revisar, instalar, configurar y dar soporte a los equipos de cómputo de propiedad del DIVRI.
c. Cumplir con los controles determinados por la DIVRI para el manejo y protección de la información.
d. Cumplir con los lineamientos definidos en los numerales 8.6.4. Equipos fuera de las instalaciones, 8.6.5. Equipos de usuario desatendido, 8.6.6. Escritorio y pantalla limpia, del presente manual.

8.3.4. Devolución de activos

Aplica lo definido en el numeral 8.2.3. Terminación o cambio de la vinculación laboral de este manual.

8.3.5. Clasificación de la información

Toda información que esté bajo responsabilidad del DIVRI debe ser identificada, clasificada y documentada con base en el procedimiento Generación Y Gestion Del Inventario De Activos De Información del DIVRI.

8.3.6. Manejo de la información en medios físicos y electrónicos

El DIVRI como propietario y custodio de la información (física o electrónica) generada como resultado del cumplimiento de su misión y visión, y acogiéndose a la normatividad que le sea aplicable para efectos de la gestión documental institucional, se reserva el derecho de su conservación o destrucción, dependiendo del nivel de

criticidad definida para la información con base en los lineamientos del Comité de Gestión y Desempeño de la DIVRI en lo referente a la Gestión Documental, la normativa establecida por el Archivo General de la Nación y el proceso de Gestión Documental.

8.3.6.1 Información en medios físicos

Para la información impresa o en medios físicos, con respecto a su acceso, uso, transporte, almacenamiento y disposición final, se aplican las directrices del Comité de Gestión y Desempeño de la DIVRI en lo referente a la Gestión Documental y los procedimientos definidos en el proceso Gestión Documental.

8.3.6.2 Información en medios electrónicos

Para la información soportada en medios electrónicos de propiedad del DIVRI, se debe:

Para la información en medios de almacenamiento como computadores, portátiles, disco duros u otros se debe:

- Mantener actualizado el inventario de los equipos que están en funcionamiento, identificando el responsable y las características del equipo, de acuerdo a lo definido en el Procedimiento gestión de capacidades TICS-P-003 V1.
- El responsable del equipo se compromete a mantener y salvaguardar la información contenida en el mismo, para el efecto debe aplicar:
- La DIVRI aplicará las técnicas de borrado seguro que se encuentren disponibles en el Proceso Estratégico Tecnologías de la Información, así mismo para el hardware dado de baja – servidores y equipos de cómputo a través del proveedor del servicio de mantenimiento preventivo y correctivo se coordinará el borrado de los discos duros de tales dispositivos

8.3.6.3. Uso y manejo de medios removibles

- La información crítica o sensible de la DIVRI que se encuentra almacenada en un medio removible cuya vida útil es menor al tiempo de retención de la información establecida por la DIVRI, el responsable del medio, deberá respaldar en otro medio para evitar la pérdida de información

- Todo medio removible es escaneado por software antivirus cada vez que sea conectado a la red interna.
- Los funcionarios y contratistas deben hacer uso de los medios de almacenamiento en nube y servidores de datos disponibles por el DIVRI, para guardar únicamente la información generada como parte de sus actividades laborales, con el fin de facilitar el acceso a la misma, es responsabilidad de los usuarios mantener la información en los almacenamientos asignados.
- Los medios removibles no son una alternativa de respaldo de información, siendo responsabilidad de los usuarios llevar la información de estos medios a los almacenamientos en nube o servido de datos para mantener la confidencialidad e integridad de la misma.
- En caso de requerirse almacenar información sensible en medios removibles, esta solo será almacenada en medios dispuestos por la DIVRI, con el acompañamiento de área de tecnología
- Es de exclusiva responsabilidad de cada funcionario tomar las medidas adecuadas para el almacenamiento y resguardo de los medios removibles, evitando accesos no autorizados, daños, pérdida de información o extravío del medio.
- Los puertos USB de los equipos de escritorio serán bloqueados por políticas del servidor de dominio, en caso de requerir habilitarlos deberá estar aprobado por la Dirección.

8.3.7. Uso de internet, correo electrónico y recursos tecnológicos

La DIVRI controla, verifica y monitorea el uso adecuado de los servicio de internet, correo electrónico y demás recursos tecnológicos. La asignación de recursos como computador o portátil a funcionarios, pasantes y contratistas, los debe gestionar el Jefe Inmediato o Supervisor del contratista o proveedor, ante el Grupo Administrativo y Financiera. La adecuación de estos recursos para la prestación del servicio la realiza el proceso estratégico tecnologías de la información. Los funcionarios, pasantes, contratistas, proveedores o partes interesadas deben hacer uso adecuado de los mismos en razón de sus funciones o actividades. El uso de internet, correo electrónico y de otros recursos tecnológicos son considerados herramientas de trabajo esenciales para las labores diarias.

8.3.8. Autenticación de usuarios

El Proceso Estratégico Tecnologías De La Información asignará un nombre de usuario, una contraseña y una cuenta de correo electrónico a funcionarios, pasantes, contratistas o proveedores o partes interesadas, previa

autorización de:

- El Proceso de Gestión Talento Humano, al ingreso del funcionario y pasante.
- El proceso de gestión contractual para los contratistas, indicando la fecha de inicio y fecha de terminación del contrato y actividad específica.
- Los Supervisores para los contratistas o proveedores que requieran tener acceso a la red del DIVRI como parte del desarrollo de su objeto contractual.

El Proceso Estratégico Tecnologías de la Información procederá a deshabilitar la cuenta de correo electrónico o acceso al servicio de aplicación asignada a funcionarios, pasantes, contratistas o proveedores o partes interesadas, previa confirmación de desvinculación del personal, por parte del proceso de gestión Talento Humano o del proceso de gestión de Contratación.

8.3.7 Correo electrónico

Consideraciones generales:

- La cuenta de correo electrónico asignada a funcionarios, pasantes, contratistas y proveedores o partes interesadas, únicamente podrá ser utilizada para finalidades relacionadas con el desarrollo de las funciones correspondientes al cargo o función u obligaciones definidas en el respectivo contrato, quedando limitado el uso de dicha cuenta al ámbito laboral y profesional.
- Los usuarios no deben utilizar una cuenta de correo electrónico que pertenezca a otra persona. En caso de ausencia temporal o vacaciones o retiro, se debe recurrir a mecanismos alternos como redirección de mensajes.
- Cualquier correo electrónico sospechoso debe ser reportado a soporte_tics@divri.gov.co.
- Los funcionarios o contratistas que tengan atribuida la gestión de cuentas de correo genéricas asociadas a determinados trámites no podrán en ningún caso hacer uso de ellas por motivos personales.
- Toda la información almacenada, gestionada o transmitida por correo electrónico de la DIVRI es propiedad del DIVRI.
- Cuando se realice el envío de información pública reservada o publica clasificada mediante correo electrónico, se aplicaran Acuerdos de Confidencialidad.

- El correo electrónico no debe ser utilizado para enviar ni recibir ni contestar mensajes o cadenas de mensajes que pudiesen causar congestión en la red de la DIVRI, o que puedan introducir códigos maliciosos o materializar riesgos de seguridad y privacidad de la información.

8.3.8. Internet

Los sitios web de DIVRI están diseñados para publicar la información de la gestión institucional, por lo tanto los funcionarios responsables de administrar o publicar contenidos en los sitios web, deberán cumplir con los requerimientos normativos y regulatorios relacionados con transparencia y acceso a la información; así mismo, no podrán publicar información diferente a la especifica del sitio web, ni información personal o de otra índole. Sin perjuicio de lo anterior, todos los usuarios que acceden a internet, tienen prohibido ingresar a los sitios presentados a continuación:

a. Sitios web relacionados con actividades de juego o apuestas;
b. Sitios web de contenido para adultos relacionados con pornografia, pedofilia o erotismo.
c. Sitios web de carácter discriminatorio, racista, o material potencialmente ofensivo, menosprecio o acoso explicito.
d. Sitios web que puedan afectar la seguridad informática, los cuales puedan poner en riesgo la disponibilidad de los servicios tecnológicos, integridad y confidencialidad de la información del DIVRI.
e. Sitios de descarga de material protegido bajo leyes de derecho de propiedad sin que se cuente con la autorización expresa o licencia de uso respectiva, o archivos electrónicos para usos no relacionados con la misionalidad del DIVRI.
f. Sitios web que inciten a la participación en cualquier actividad ilegal o criminal.
g. Sitios de descarga o visualización de películas, juegos entretenimiento.

El personal del DIVRI que como parte del desarrollo de las actividades misionales requiera el acceso a un sitio web relacionado con una de las categorías anteriores, deberá previamente justificar la necesidad y obtener la autorización formalizada por parte del jefe inmediato o supervisor del contrato, solicitar a la al proceso estratégico tecnologías de la información la habilitación del acceso al sitio web especificado por tiempo limitado.

8.4. CONTROL DE ACCESO

8.4.1. Política para el control de acceso

El DIVRI implementa los controles de acceso a la información por parte de funcionarios, pasantes, contratistas y proveedores o partes interesadas, conforme al perfil de acceso establecidos en los sistemas de información o bases de datos, así mismo garantiza la implementación de controles de seguridad física e informática para la protección de las instalaciones de procesamiento de información y cualquier otra área considerada crítica para la operación de la DIVRI.

Usuarios: Los usuarios del DIVRI son todos los funcionarios, pasantes, contratistas, proveedores.

Usuarios de consulta: Usuarios de la DIVRI, entidades públicas y privadas, ciudadanos y demás partes interesadas, que estén relacionadas de forma temporal o permanente con la DIVRI.

8.4.2. Acceso a redes y a servicios de red

El acceso a la red de datos del DIVRI se realiza con el nombre de usuario y contraseña asignados por el Proceso Estratégico Tecnologías de la Información a funcionarios, pasantes, contratistas y proveedores, o partes interesadas quienes deben proteger y no compartir sus credenciales de acceso a la red y servicios de red (correo electrónico, red inalámbrica, aplicaciones, entre servicios tecnológicos) que le son conferidos de acuerdo con su perfil. Los funcionarios son responsables de su nombre de usuario y contraseña asignados, así como notificar a la Proceso Estratégico Tecnologías de la Información el cambio de su contraseña cuando se sospeche el conocimiento de ésta por terceras personas.

La DIVRI dispondrá en cada vigencia los recursos necesarios la correcta operación de la infraestructura tecnológica de red.

EL Proceso de Tecnologías de la Información esta encargada de administrar la infraestructura de red y proporcionar la configuración necesaria para el cumplimiento de las funciones y/ actividades de cada área.

EL Proceso de Tecnologías de la Información contará con mecanismos de seguridad que otorguen la protección necesaria ante amenazas y permita control del tráfico de entrada y de salida para la red LAN de la entidad.
EL Proceso de Tecnologías de la Información, mantendrá segmentada la red por centros de cableado y acceso WIFI.

8.4.3. Administración de cuentas de usuario y contraseñas

Los funcionarios, pasantes, contratistas, proveedores o partes interesadas, deben cumplir con las políticas para el uso de cuentas de usuario y contraseñas, relacionadas con la responsabilidad de cualquier acción que se realice utilizando la cuenta de usuario y contraseña asignada, así mismo se deberá tener en cuenta lo siguiente:

a. Las cuentas de usuario y contraseñas se establecen de acuerdo con los estándares y directrices definidas por el Proceso Estratégico Tecnologías de la Información, con el propósito de que no sean fáciles de descifrar.
b. Las cuentas de usuario y contraseñas son de uso personal e intransferible y por ningún motivo se deben prestar o facilitar a otros funcionarios, pasantes, contratistas, proveedores o partes interesadas.
c. Las cuentas de usuario y contraseñas no deben ser reveladas por vía telefónica, correo electrónico, o ser escritas en ningún medio, excepto cuando son entregadas en custodia, previa autorización del Jefe inmediato del funcionario o contratista y del Proceso Estratégico Tecnologías de la Información.
d. No se debe habilitar la opción "recordar clave en este equipo", que ofrecen los programas o aplicaciones o navegadores web, esto con el fin de limitar el acceso a los aplicativos a personas no autorizadas, especialmente para los funcionarios, pasantes, contratistas, proveedores o partes interesadas con acceso remoto autorizado a la plataforma tecnológica y aplicativos o sistemas de información de la DIVRI.
e. Reportar al correo electrónico soporte_tics@DIVRI.gov.co, cualquier sospecha de uso no autorizado del usuario y contraseña asignados.

8.5. CRIPTOGRAFÍA

8.5.1. Política sobre el uso de controles criptográficos

En el DIVRI no se permite el uso de herramientas o mecanismos de encripción o de firmas digitales diferentes a las definidas y autorizadas por el Proceso Estratégico Tecnologías de la Información.

8.5.2. Gestión de certificados de firma digital

El DIVRI dispone de la infraestructura tecnológica necesaria para soportar la operación de certificados de firma digital.

La Oficina de Sistemas de Información administra la plataforma para la gestión de los certificados de firma digital para los aplicativos que implementan dicha funcionalidad. Los funcionarios y contratistas deben informar cualquier evento o incidente relacionado con el uso de la firma digital asignada al correo electrónico soporte_tics@DIVRI.gov.co.

8.6. SEGURIDAD FÍSICA Y AMBIENTAL

8.6.1. Áreas seguras

La DIVRI cuenta con los mecanismos de control de ingreso y acceso físico a las instalaciones de la DIVRI por parte de funcionarios, pasantes, contratistas, proveedores o partes interesadas, los cuales por el Grupo Administrativo y Financiero con el proveedor del servicio de vigilancia a instalaciones.

El ingreso a las instalaciones del DIVRI y el acceso a las áreas seguras como son Gestión Documental y bodegas por parte de funcionarios, pasantes, contratistas, proveedores o partes interesadas, deben ser autorizados por el funcionario responsable del área física específica o Supervisor del contratista o proveedor de acuerdo al alcance de la actividad que se requiera adelantar y deben ser acompañados por un funcionario del área durante el tiempo que dure la visita o actividad.

El ingreso a los centros de cómputo, centros de cableado y áreas de ingreso restringido del DIVRI solo está autorizado a personal técnico que desarrolla trabajos técnicos en estas áreas. El acceso será autorizado por el Coordinador del Grupo Administrativo y Financiero de acuerdo al alcance de la actividad que se requiera adelantar y deben ser acompañados por un funcionario del área durante el tiempo que dure la visita o actividad.

8.6.2. Seguridad de equipos

La DIVRI cuenta con controles que le permiten monitorear la disponibilidad e integridad de la infraestructura tecnológica, así como los niveles adecuados de mantenimiento y soporte a la infraestructura de red, plataformas operativas, sistemas de información, aplicativos, aseguramiento de servidores, entre otros. En caso de pérdida o robo del dispositivo móvil de propiedad de la DIVRI, el responsable del dispositivo reporta inmediatamente el hecho al Jefe inmediato, Grupo Administrativa y al Grupo de Ingeniería y Soporte Técnico, y de inmediato se realizan las siguientes acciones:

- Inhabilitar los servicios asociados al dispositivo.
- Las credenciales son modificadas.
- Se notifica a los grupos de interés donde potencialmente se pudieron haber comprometido activos de información

8.6.3. Ingreso o retiro de activos

La DIVRI aplica los controles para el registro de entrada y salida de las instalaciones de la DIVRI de personas, equipos y elementos. El ingreso o retiro de los equipos de cómputo por parte de los funcionarios o contratistas deberá quedar registrado en la recepción del piso o bodega desde el cual se realice la entrada o salida. El ingreso o retiro de información debe ser autorizado por el propietario de la información – Líder o responsable de proceso, quien deberá informar al Proceso de Gestión Tecnologías de la Información para aplicar los controles para el almacenamiento, transporte o transferencia de la información desde o hacia otras organizaciones.

8.6.4. Equipos fuera de las instalaciones

Los funcionarios que desarrollan sus funciones en sitio o en modalidad de teletrabajo y contratistas en modalidad de trabajo remoto, con asignación de computadores, portátiles, o Tablets de propiedad del DIVRI, son responsables y custodios del bien asignado, así como de la información que en el dispositivo se encuentre almacenada, para lo cual deben tener en cuenta que: Los equipos portátiles son para uso exclusivo de las funciones asignadas por la DIVRI y no deben ser manipulados por personas diferentes a los responsables, como se dispone en el numeral 8.3.3. Uso adecuado de los activos y recursos de información del presente Manual.

8.6.5. Equipos de usuario desatendido

Los servidores, computadores y portátiles tendrán habilitado el control automático de bloqueo de sesión. Por defecto el bloqueo se habilita después de diez (10) minutos de inactividad, y solo se podrán desbloquear con el usuario y contraseña asignada.

Los funcionarios, pasantes, contratistas, proveedores o partes interesadas con equipos asignados por el DIVRI, deben bloquear su computador o portátil cada vez que se retiren temporalmente de su lugar de trabajo y una vez finalizada su jornada laboral deben apagarlo. Los computadores y portátiles del DIVRI solo deben mostrar en el escritorio de pantalla el papel tapiz o fondo de pantalla o protector de pantalla institucional, o el definido para comunicar temas de interés institucional, de acuerdo con el protocolo de comunicaciones del DIVRI.

8.6.6. Escritorio y pantalla limpia

El DIVRI promueve:

a. La política de escritorio limpio en los lugares de trabajo para proteger la información crítica o sensible en medios impresos.
b. La política de pantalla limpia en computadores, portátiles y servidores, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Los funcionarios, pasantes, contratistas, proveedores o partes interesadas deben tener en cuenta las siguientes consideraciones:

a. En los lugares de trabajo solo deben permanecer los documentos y elementos necesarios para la realización de las labores. No se deben dejar documentos originales, preliminares o finales con información reservada o clasificada a la vista de otras personas, o desatendidos en otro lugar diferente al sitio de trabajo. Las copias de trabajo deben ser destruidos antes de ser arrojados a la basura. No se deben reutilizar documentos impresos que contengan información reservada o clasificada.
b. Se debe aplicar los controles de seguridad y privacidad de la información para los activos sensibles y críticos determinados por el DIVRI con el fin de salvaguardar la información reservada o clasificada que se encuentre en cualquier medio.

c. Realizar La liberación de los trabajos de impresión o de escáner de documentos evitando desperdicios de papely consumos de tonner.

8.7. SEGURIDAD DE LAS OPERACIONES

8.7.1. Procedimientos de operación documentados

Se tienen establecidos los procedimientos, registros e instructivos de trabajo debidamente documentados, con el fin de asegurar el mantenimiento y operación adecuada del DIVRI. Todas las tareas relacionadas con el mantenimiento de la infraestructura tecnológica, del centro de cómputo, de computadores, portátiles, plantas eléctricas, aire acondicionado y demás dispositivos, se realiza de forma programada, es comunicada su ejecución y documentada.

8.7.2 Gestión de capacidad

El proceso de Tecnologías de la Información aplica el procedimiento Gestión de la Capacidad de TI, con el objeto de garantizar la disponibilidad de los recursos tecnológicos requeridos por los procesos del negocio. Para lo cual tiene en cuenta:

a. La identificación de necesidades a nivel tecnológico, con el fin de evitar potenciales indisponibilidades de los servicios de tecnológicos y de aplicación, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y así mismo permita planificar una adecuada acción correctiva.
b. La definición del cambio, la transición o cierre definitivo de las aplicaciones, sistemas de información, bases de datos, equipos o ambientes.

8.7.3. Protección contra códigos maliciosos

El proceso de Tecnologías de la Información dispondrá de herramientas de seguridad antimalware y antispam debidamente licenciadas, que minimizan el riesgo de contagio de software malicioso.

Los servidores públicos, contratistas y pasantes no deben cambiar o eliminar la configuración del software antimalware configurada en los equipos de cómputo de propiedad de la DIVRI. Solamente pueden realizar tareas de escaneo de virus en diferentes medios de almacenamiento.

Los equipos de cómputo de propiedad de los contratistas deben contar con un software de antimalware licenciado y actualizado.

Cuando el software de antimalware notifique que el equipo de cómputo o archivo se encuentra infectado, es responsabilidad de los servidores públicos, contratistas y pasantes notificar el evento a soporte_tics@divri.gov.co.

En caso de detectar o sospechar que el equipo de cómputo se encuentra infectado por software malicioso, es responsabilidad de los servidores públicos, contratistas y pasantes informar el evento a soporte_tics@divri.gov.co esta situación, para que se tomen las medidas pertinentes.

8.7.4. Copias de respaldo

El Proceso de Tecnologías de la Información realiza copias de respaldo para la información crítica de la DIVRI contenida en los servidores y en las bases de datos de los sistemas de información y aplicativos del DIVRI. Los funcionarios y contratistas son responsables de realizar las copias de seguridad o de backup de la información almacenada en los computadores y portátiles asignados en los medios de almacenamiento dispuestos por el DIVRI.

8.8. SEGURIDAD DE LAS COMUNICACIONES

8.8.1. Controles de redes y seguridad de los servicios de red

El proceso de Tecnologías de la Información es la responsable de implementar los protocolos de seguridad e la infraestructura de red local, que permitan acceder a los recursos de manera segura.

Con el propósito de proteger los equipos de cómputo, equipos de comunicaciones y demás dispositivos tecnológicos de la

DIVRI, no se permite la conexión a la infraestructura de red local de la entidad a los equipos de cómputo y de comunicaciones propiedad de terceros sin previa autorización del director, jefe, coordinador o supervisor de contrato, mediante la solicitud realizada por medio del Sistema de Mesa de Servicio.

Los servidores públicos, contratistas y pasantes pueden acceder a la infraestructura red local de la entidad a través de conexión LAN y WIFI, utilizando el equipo de escritorio o portátil asignado por la entidad, el usuario asignado y clave.

Se pueden conectar a los recursos de conexión remota – VPN los servidores públicos y contratistas previamente autorizados por el director, solicitud que debe realizarse a través de la Sistema de mesa de servicio del proceso de Tecnologías de la Informacion.

8.8.2. Separación en las redes

La plataforma tecnológica del DIVRI está distribuida en segmentos de red independientes - VLANs -, separando las redes de servicios internos de la DIVRI, de las conexiones con terceros y del acceso a Internet.

8.8.3. Transferencia de información

El intercambio de información reservada o clasificada del DIVRI con proveedores y partes interesadas está amparado mediante decretos, convenios o acuerdos de confidencialidad, que garanticen los controles requeridos para asegurar la integridad y confidencialidad de la información.

Convenios de interoperabilidad y transferencia de información:

La transferencia e intercambio de información para propósitos de interoperabilidad con grupos de valor se realiza conforme con la normatividad vigente
Las condiciones técnicas para el intercambio de información deben ser definidas y aprobadas por el proceso de Tecnologías de Información, Las condiciones administrativas para el intercambio de información deben ser definidas y aprobadas por el líder del proceso responsable del intercambio de información con el grupo de valor el cual se compartirá la información. Para el intercambio seguro de información se aplican los lineamientos de seguridad para interoperabilidad definidos por el Ministerio de las Tecnologías de Información y las Comunicaciones.

8.9. GESTIÓN DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Proceso de Tecnologías de la Información aplica el Procedimiento Gestion de Incidentes de seguridad de la Información GTICS-P-002 V1. para dar respuesta oportuna a los eventos e incidentes que puedan impactar de forma negativa los activos de información DIVRI.

Para la adecuada gestión de los incidentes de seguridad y privacidad de la información se debe:

a. Los funcionarios, pasantes, contratistas, proveedores y partes interesadas deben reportar al correo electrónico soporte_TICS@DIVRI.gov.co cualquier situación, evento o escenario que evidencie un riesgo materializado, amenaza o vulnerabilidad detectada en los servicios de aplicación o tecnológicos y que pueden tener impacto en la seguridad y privacidad de la información en los sistemas de información o los servicios tecnológicos de la DIVRI.
b. Las amenazas reportadas por los equipos de seguridad perimetral son tratadas acorde con el 2. Procedimiento Gestion de Incidentes de seguridad de la Información GTICS-P-002 V1.

8.10. CUMPLIMIENTO DE REQUERIMIENTOS

8.10.1. Cumplimiento de las obligaciones legales

La DIVRI da cumplimiento a las normas y regulaciones relacionadas con:

a. La gestión de la seguridad y privacidad de la información en procesos, en el entorno de información y comunicación institucional y el entorno tecnológico.
b. La salvaguarda en los contratos y convenios mediante la suscripción de compromisos o acuerdos de confidencialidad sobre el manejo de la información institucional en cualquiera de sus formas.
c. El uso y publicación de documentos creados en la DIVRI, así como los otorgados por terceros que se requieran para documentar las actividades de la misión institucional.

8.10.2. Derechos de propiedad intelectual

El cumplimiento de las normas de propiedad intelectual emitidas por la Dirección Nacional de Derechos de Autor, relacionadas con los Derechos de Autor para el Uso de Software, material filmico, fotográfico, de audio o de

derechos conexos, cuenta en el DIVRI con los procedimientos, mecanismos y controles para garantizar el cumplimiento de las restricciones legales al uso del material protegido, así:

- La DIVRI solo podrá autorizar el uso de material (documentos, fotografías, videos, audios) producidos como parte del ejercicio misional, o haciendo uso de material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas con los proveedores y conforme lo dispuesto por la normativa vigente.
- La DIVRI conserva las pruebas y evidencias de propiedad de licencias de software y de material documental producido o con autorización de uso por terceros.
- La DIVRI verifica que sólo se instalen en sus equipos productos con licencia y software autorizado.
- La DIVRI da cumplimiento a las normas, regulaciones y demás directrices que emita el gobierno nacional para el uso de software por parte de los entes Estatales

8.10.3 Privacidad y protección de información de datos personales

La DIVRI en cumplimiento de las normas y regulaciones para la protección de los datos personales cuenta con la Política de Protección de Datos Personales

8.10.4 Revisiones de seguridad de la información

La DIVRI asegura el cumplimiento de las políticas de seguridad y privacidad de la información en sus procesos institucionales.

REVISADO Y APROBADO

	ELABORADO	REVISADO (Coordinador)	REVISADO (Planeación)	APROBADO (Director)
Nombres y Apellidos Grado y Cargo	Yeny Aracelly Nuñez Rosero	GR(R) Andrea del Pilar Diaz Rodriguez	Paola M. Calderón Pérez	MY(R) Juan Carlos Barrera Medina

Fecha	Profesional Defensa- TIC	Coordinadora Administrativa y Financiera	Asesor Defensa – Área de Planeación	Director de Veteranos y Rehabilitación Inclusiva
	17-AGO-2023	17-AGO-2023	17-AGO-2023	17-AGO-2023

CONTROL DE CAMBIOS

VERSIÓN	ACCIÓN	DESCRIPCIÓN DE LA ACCIÓN	FECHA	RESPONSABLE
01	Creación	Versión Inicial del documento de política de seguridad y privacidad de la información, conforme a lo establecido en la sesión del Comité de Gestión y Desempeño Institucional del 16 de agosto de 2023	17 AGO 2023	Paola M. Calderón Pérez