1.PROCESO: TIC									
2.TIPO DE PROCESO	**Estratégico**		**Misional**		**Apoyo**	**x**	**Seguimiento y evaluación**		
3. OBJETIVO	Adoptar la resolución 7870-2022 Por la cual se emite y adopta la Política General de Seguridad y Privacidad de la información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos en las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa, y se dictan otras disposiciones.								
4.RESPONSABLE	Todos los procesos de la DIVRI								
5. ALCANCE	la Política de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de la Operación y define lineamientos frente al uso y manejo de la información en las Unidades Ejecutoras del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas del Sector Defensa y seguridad incluyendo la Unidad Administrativa Especial de la Justicia Penal Militar y Policial en adelante Sector Defensa, de acuerdo al ARTÍCULO 1. Y 3 De la resolución 7870-2022. Serán sujetos obligados de la presente resolución todos los niveles de las entidades del Sector Defensa, todos sus funcionarios, contratistas, proveedores, operadores y terceros que en razón del cumplimiento de sus funciones compartan, utilicen, recolecten, procesen, intercambien o consulten información del Ministerio de Defensa Nacional, así como los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independiente de su ubicación. Esta política también se aplicará a toda la información creada, procesada o utilizada por el Ministerio, sin importar el medio, formato o presentación o el lugar en el cual se encuentre.								
6. DEFINICIONES	**Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4). **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).								

Activos de Información y recursos: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)**Amenazas:** causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/ IEC 27000).
Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa almacena y transporta mediante los sistemas de información que se encuentran interconectados.
Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (ISO/IEC 27000).
Contenido digital: corresponde a cualquier pieza de información que podemos incluir en un medio digital. Pueden estar formados por textos, imágenes, vídeos, mapas entre otros.
Control: 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 es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las Entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6). **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3). **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3). **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h) **Datos Personales Mixtos:** Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles. **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3). **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional). **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (ISO/IEC 27000). **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio

	con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3). **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (1S0/IEC 27000). **Incidente:** Un incidente de seguridad de la información puede definirse también como cualquier evento que tenga el potencial de afectar la preservación de la confidencialidad, integridad, disponibilidad o valor de la información. **Información electrónica:** Es todo dato conservado en un formato electrónico el cual permite su tratamiento automático tratándose por regla general de soportes electrónicos. **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6) **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6). **Integridad:** Propiedad de la información relativa a su exactitud y completitud. (ISO/IEC 27000). **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008. **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014. **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado. (Modelo de Seguridad y Privacidad de la Información - Ministerio de Tecnologías de la Información y las Comunicaciones) **No repudio:** Es un concepto que garantiza que alguien no puede negar algo. En el contexto de la seguridad de la información, normalmente el no rechazo se refiere a la capacidad de garantizar que una parte de un contrato o una comunicación no pueda negar la autenticidad de su firma en un documento o el envío de un mensaje enviado por un origen determinado. (ISO/IEC 27000). **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000). **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000). **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan

	en el país. (Ley 1581 de 2012, art 25) **Responsabilidad Demostrada:** Conducta desplegada por los responsables o encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias. (Modelo de Seguridad y Privacidad de la Información - Ministerio de Tecnologías de la Información y las Comunicaciones) **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3). **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000). **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000). **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales. (Modelo de Seguridad y Privacidad de la Información - Ministerio de Tecnologías de la Información y las Comunicaciones) **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3) **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3). **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. (ISO/IEC 27000). **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000). **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad. (Modelo de Seguridad y Privacidad de la Información - Ministerio de Tecnologías de la Información y las Comunicaciones)

8. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CAPITULO	ARTICULOS	DESCRIPCION
	CAPÍTULO I DISPOSICIONES GENERALES	**ARTÍCULO 2. Lineamientos Generales de Seguridad y privacidad de la Información, Seguridad digital, Ciberseguridad y Continuidad de la Operación.**	El Ministerio de Defensa Nacional, protege, preserva y administra la confidencialidad, integridad, disponibilidad y autenticidad de la información, así como la seguridad digital, ciberseguridad y gestión de la continuidad de la operación, conforme a los procesos de cada una de las entidades, dando cumplimiento a los requisitos legales y reglamentarios; previniendo igualmente los incidentes mediante la gestión de riesgos integrales en seguridad y privacidad de la información, seguridad digital, ciberseguridad y la implementación de controles de seguridad físicos y digitales, orientados a la mejora continua en la gestión y el alto desempeño del Sistema de Gestión de Seguridad de la Información.
		ARTÍCULO 4. Objetivos.	La Política de Seguridad y Privacidad de la Información, Seguridad digital, Ciberseguridad y Continuidad de la Operación, tendrá los siguientes objetivos: a. Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la información en el Sector Defensa. b. Definir los lineamientos necesarios para mitigar los incidentes y gestionar los riesgos y controles de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de la Operación en el Sector Defensa de acuerdo a las normas vigentes. c. Emitir los lineamientos necesarios para el manejo de información y de los recursos tecnológicos del Sector Defensa.

		ARTÍCULO 6. Misión General.	**ARTÍCULO 6. Misión General.** El Ministro de Defensa Nacional, emite la presente resolución, con el fin de estandarizar la Política General de Seguridad y Privacidad de la información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios tecnológicos para todas las entidades que conforman el Sector Defensa, las cuales se dictan en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, de los sistemas informáticos y de los ambientes tecnológicos. Estas políticas, deberán ser conocidas, difundidas y cumplidas por todo el personal que tenga relación con activos de información del Sector Defensa. **PARAGRAFO. Misiones Particulares.** El comandante General de las Fuerzas Militares, los Comandantes de Fuerza, el Director General de la Policía Nacional, los Viceministros y Directores, Gerentes, Superintendentes o similares de entidades del Sector Defensa deberán:	
			a. Verificar el cumplimiento de la presente resolución y demás normas que la desarrollen, adicionen o modifiquen.	
			b. Promover la adopción de medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital.	
			c. Promover el desarrollo de una cultura de seguridad de la información y ciberseguridad a través de campañas de sensibilización y concientización.	
			d. Adoptar la seguridad digital y ciberseguridad con un enfoque preventivo y proactivo, priorizando la protección de datos personales e información sensible de la entidad o que goza de reserva legal, al igual que los servicios y sistemas de información e infraestructura críticas.	

			e. Fungir como único canal de comunicación autorizado para hacer pronunciamientos oficiales ante entidades externas, medios de comunicación o la ciudadanía, reportará los incidentes que afecten la infraestructura crítica y la Seguridad Nacional ante las autoridades competentes.	
			f. Designar mediante acto administrativo al servidor público Responsable de Seguridad de la Información representante de la Alta Dirección para el Modelo de Seguridad y Privacidad de la Información (MSPI), con el fin de apoyar las actividades y controles necesarios para llevar a cabo la implementación y la mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI) en su entidad.	
			g. Gestionar los recursos financieros requeridos para la implementación del (MSPI).	
			h. Ordenar la inclusión, de ternas relacionados con seguridad de la información y ciberseguridad, en las materias y cursos de tecnología que se dictan en las escuelas de formación y capacitación de las Fuerzas Militares y Policía Nacional.	
			i. Apoyar la creación de los respectivos Equipos de Respuesta a Emergencias Informáticas (CSIRT) y Centros de Operaciones de Seguridad (SOC), con el propósito de apoyar a la gestión de incidentes.	

	CAPÍTULO II POÚTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL, CIBERSEGURIDAD Y CONTINUIDAD DE LA OPERACIÓN	**ARTÍCULO 7. Política de Privacidad y tratamiento de datos personales.**	Para el tratamiento de la información de todas las personas, que en algún momento por razones de la actividad que desarrollan, hayan suministrado datos personales a las entidades del sector Defensa, así corno la información de los funcionarios y contratistas que participan en el desarrollo de las funciones de las mismas; el Sector Defensa, cuenta con la "Política de tratamiento de Datos Personales en el Ministerio de Defensa Nacional' que se encuentre vigente, dando cumplimiento a lo dispuesto por el Gobierno Nacional y las demás normas externas que los modifiquen, adicionen o complementen. Así mismo cada entidad deberá aplicar las Políticas de Datos Personales particulares que le apliquen dependiendo de su rnisionalidad y naturaleza jurídica. **PARAGRAFO.** El responsable de la protección de datos personales o quien ejerza sus funciones en las entidades del Sector Defensa, velará por el cumplimiento de las normas de protección de datos personales expuestas anteriormente y aquellas que se adicionen, modifiquen o sustituyan.	
		ARTÍCULO 8. Políticas de Seguridad de la Información.	**ARTÍCULO 8. Políticas de Seguridad de la Información.** Las Direcciones de Tecnología de las entidades del Sector Defensa o quien haga sus veces, deberán definir e implementar una estrategia de seguridad digital y ciberseguridad en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información a través del habilitador de seguridad y privacidad de la información en el marco de la Política de Gobierno Digital, de conformidad con el Modelo de Seguridad y Privacidad de la Información (MSPI) y de acuerdo a los lineamientos sectoriales de política de seguridad de la información emitidos en la Directiva Permanente Ministerial DIR2014-18, en todos los procesos, trámites, sistemas de información, infraestructura tecnológica e infraestructura critica, para prestar servicios de confianza, generando protección de la información de los ciudadanos, gestionando los riesgos y los incidentes de seguridad digital y ciberseguridad. PARAGRAFO 2. Es responsabilidad de los lideres de proceso en las entidades del Sector Defensa, definir, documentar, mantener, actualizar y mejorar permanentemente los procedimientos relacionados con sus procesos, incluyendo aquellas actividades que sean consideradas como controles de	

			Seguridad de la Información dentro de dichos procedimientos, y en coordinación con la Dirección de Tecnología o quien haga sus veces en las entidades del Sector Defensa.	
		ARTÍCULO 9. Política de Seguridad de los Recursos Humanos.	La dependencia de Talento Humano con el apoyo de la Dirección de Tecnología o las que hagan sus veces en las entidades del Sector Defensa desplegarán esfuerzos para que los servidores públicos conozcan sus responsabilidades frente a la seguridad de la información, seguridad digital y ciberseguridad, con el fin de reducir el riesgo por hurto de medios informáticos, acceso abusivo a los sistemas informáticos, daño informático y de aseguramiento de la confidencialidad, disponibilidad e integridad de la información. PARÁGRAFO. En cumplimiento de este artículo, las dependencias de Talento Humano, o las que hagan sus veces de entidades del Sector Defensa, deberán:	
			• Incluir en los programas de inducción y de reinducción el tema de seguridad de la información asegurando que los funcionarios conozcan sus responsabilidades, así como las implicaciones por el uso indebido de activos de información o de otros recursos informáticos, haciendo énfasis en las consecuencias jurídicas que puede acarrear al servidor público; de tal forma que ante incidentes de seguridad digital, que generen conductas punibles, tipificadas como tal por la legislación penal, se deberá priorizar la realización de la respectiva denuncia ante las autoridades competentes de realizar su investigación y en el marco de los procedimientos que para el efecto dispongan los órganos de policía judicial.	
			• Incluir en el Plan Institucional de capacitaciones PIC, o el que haga sus veces, actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que ésta considere relevantes para mejorar habilidades y promover conciencia en la seguridad de la información, seguridad digital y gestión de riesgos.	

			• Las dependencias de Contratación o las que hagan sus veces, incluirán en las minutas de los contratos, cualquiera que sea la modalidad, cláusulas y obligaciones tendientes a la seguridad de la Información y serán divulgadas a los contratistas a través de los supervisores, con el fin de reducir el riesgo de robo, fraude, mal uso de las instalaciones y medios, asegurando la confidencialidad e integridad de la información.	
			• Los servidores públicos, contratistas, estudiantes y terceros, como parte de sus términos y condiciones iniciales de trabajo, cualquiera que sea su nivel jerárquico dentro de la entidad, a través de las áreas de Talento Humano y contratación respectivamente firmarán el documento de compromiso de confidencialidad y no divulgación de acuerdo al tratamiento de información de la entidad y de datos personales en los términos de la Ley 1581 de 2012, capítulo 25 del Decreto 1074 de 2015 y Ley 1712 de 2014, reglamentada por el Decreto 1081 de 2015 capitulo 2 y las demás normas que las adiciones, modifiquen, reglamenten y complementen. Igualmente, en el mismo documento declararán conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo, esto con garantía de respeto al derecho a la privacidad.	
		ARTÍCULO 10. Política de Gestión de Activos de Información.	**ARTÍCULO 10. Política de Gestión de Activos de Información**. Las entidades del Sector Defensa a través de sus Direcciones de Tecnología o quienes hagan sus veces, apoyadas en las áreas de Seguridad Digital y Ciberseguridad o las que hagan sus veces, establecerán y divulgarán los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información con el objetivo de garantizar su protección, teniendo en cuenta:	

			a. **Inventario de Activos de Información.** En cada una de las entidades se debe llevar el inventario de los activos de información de tal manera que sean identificados, clasificados, valorados y controlados para garantizar su uso adecuado, protección, recuperación ante desastres y continuidad del negocio. Para ello se pueden apoyar en la Guía No. 5 para la Gestión y Clasificación de Activos de información emitida por MinTIC. Así mismo, se debe realizar la valoración de riesgos de los activos de información de acuerdo con lo establecido en el ARTICULO 20. Para establecer los controles de seguridad físicos y digitales, las dependencias que tienen la custodia de la información generada de acuerdo con su función se encargarán de proteger la información, software, hardware y recurso humano, así como mantener actualizado el inventario de activos de información relacionados con sus servicios.	
			b. **Activos de Gestión documental.** La Dirección Administrativa o quien haga sus veces a través del grupo o dependencia de archivo documental o similar y con la asesoría del responsable de seguridad de la información o quien haga sus veces, deberá implementar los controles necesarios para que los archivos de gestión documental cuenten con los mecanismos de seguridad que propendan por la protección contra amenazas internas, externas y ambientales que permitan la conservación, integridad, confidencialidad y disponibilidad de la información. Para retención y destrucción final de la información digital o en físico, se deben establecer procesos y procedimientos de acuerdo con las tablas de retención documental dispuestas por el Archivo General de la Nación.	
			c. **Clasificación de la Información.** Las entidades del Sector Defensa deben clasificar la información física, electrónica y digital de acuerdo con lo definido en la Ley 1712 de 2014 por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.	

			d. **Incidentes de Seguridad:** Gestionar la solución de los incidentes relacionados con el acceso no autorizado o mala utilización de los activos de información bajo su responsabilidad, incluyendo los incumplimientos a la disponibilidad, confidencialidad e integridad.	
			PARÁGRAFO. Preservación Documental. La Dirección Administrativa o quien haga sus veces a través del grupo o dependencia de archivo documental con la asesoría del responsable de la seguridad de la información o quien haga sus veces, deberá implementar los controles necesarios para que la gestión documental (gestión, central e histórico) cuente con los mecanismos de seguridad que garanticen su protección, conservación, integridad, confidencialidad, disponibilidad desde la recepción y radicación hasta los procesos de disposición final de los documentos de acuerdo con las Tablas de Retención Documental y Tablas de Valoración Documental.	
		ARTÍCULO 11. Política de Control de Seguridad Física y lógica.	**ARTÍCULO 11. Política de Control de Seguridad Física y lógica.** Con el fin de mitigar riesgos asociados al acceso a la información, infraestructura tecnológica e infraestructura física de personal no autorizado, y así propender por salvaguardar la integridad, disponibilidad y confidencialidad de la información, se deberán implementar las siguientes acciones:	
			• Los propietarios de los activos de información o las dependencias responsables en coordinación con las Dirección de Tecnologías de las entidades del Sector Defensa o quien haga sus veces y teniendo en cuenta el tipo de activo, establecerán medidas de control de acceso lógico y físico teniendo en cuenta la autenticación de múltiples factores a nivel de red, sistema operativo, sistemas de información, servicios de tecnología e infraestructura física (instalaciones y oficinas).	

			• Adoptar las medidas para la protección del perímetro de seguridad de sus instalaciones físicas, para control de acceso y permanencia del personal en las oficinas, instalaciones, y áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información reservada, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones); así mismo tomar las medidas necesarias para mitigar los riesgos y amenazas externas y ambientales, con el fin de evitar afectación a la confidencialidad, disponibilidad e integridad de la información del Ministerio.
		ARTÍCULO 12. Política de Seguridad de las Comunicaciones.	**ARTÍCULO 12. Política de Seguridad de las Comunicaciones**. Las Direcciones de Tecnología o quien haga sus veces o la dependencia encargada en las entidades Sector Defensa deberán:
			•Establecerlos mecanismos necesarios para proveer la disponibilidad de las redes y de los servicios que dependen de ellas; así mismo, dispondrá de los mecanismos necesarios de seguridad para proteger la integridad y la confidencialidad de la información.
			• Definir mecanismos para que el intercambio de información con los grupos de interés internos o externos se realice asegurando su integridad, de conformidad con las normas vigentes sobre la materia.
			• Realizar los controles criptográficos definidos en el literal c, del artículo 16 de la presente Resolución para los casos en que los acuerdos de intercambio de información requieran del desarrollo de Web Services o cualquier otro medio tecnológico.
			• Implementar controles y procesos que habiliten la integración al servicio ciudadano digital de interoperabilidad de forma segura y cumpliendo

		ARTÍCULO 13. Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.	**ARTÍCULO 13. Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.** Las Direcciones de Tecnología o quien haga sus veces, serán las únicas dependencias con la capacidad de adquirir, desarrollar e implementar o avalar la adquisición, desarrollo y mantenimiento de los sistemas de información y comunicaciones, conforme a las políticas y requerimientos establecidos en las entidades del Sector Defensa, con el acompañamiento de las oficinas responsables de la contratación en cada entidad del Sector Defensa.	
			Igualmente deberá contemplar lo concerniente a seguridad digital y ciberseguridad para todos los sistemas de información, aplicaciones web y móviles, así como cualquier otro sistema que almacene, transmita o presente información, desde las etapas iniciales como el diseño y levantamiento de requerimientos, hasta las pruebas de vulnerabilidad, una vez el software se encuentre en producción, teniendo en cuenta los riesgos asociados a cada sistema de información. Dicho proceso deberá quedar documentado y estar alineado con las normas de responsabilidad demostrada en el tratamiento de datos personales definidos en el artículo 6 de la presente resolución.	
			PARÁGRAFO 1. Cualquier software o aplicativo que opere en las entidades del Sector Defensa deberá reportarse y entregarse a las Direcciones de Tecnología o quien haga sus veces, cumpliendo con los lineamientos técnicos y presupuestales con el fin de salvaguardar la información, brindar el soporte, y demás procesos técnicos que permita su recuperación en caso de algún incidente o siniestro.	
			PARÁGRAFO 2. Para asegurar que la adopción, implementación de tecnologías de nube sea confiable y segura, toda adquisición que contemple un servicio ya sea de hardware o software con tecnologías en la Nube, deberá aplicar lo consignado en la Resolución 463 del 9 de febrero de 2022.	

			PARÁGRAFO 3. Los servidores públicos y contratistas responsables de la calidad de la información ingresada en los diferentes sistemas de información usados en las entidades del Sector Defensa, deberán alimentar los datos que son editables en forma íntegra y veraz.
		ARTÍCULO 14. Política de Seguridad para Relación con Proveedores.	**ARTÍCULO 14. Política de Seguridad para Relación con Proveedores.** Las entidades del Sector Defensa, a través de las respectivas dependencias de Contratación, propenderán que en sus procesos de contratación se identifiquen riesgos y controles necesarios en la relación con los proveedores de las respectivas entidades.
			PARÁGRAFO 1. Las Direcciones de Tecnología o quien haga sus veces asegurarán que la información a la que tengan acceso los proveedores, cumpla con lo establecido en el marco de la seguridad y privacidad de la información; para lo cual: • Establecerán mecanismos de control de acceso a la información e infraestructura tecnológica en la relación con sus proveedores.
			• Monitorearan y evaluaran los procesos o actividades sobre las plataformas tecnológicas, delegados en terceros.
			PARÁGRAFO 2. El supervisor de cada contrato o convenio será responsable de divulgar las políticas y procedimientos de seguridad de la información.
		ARTÍCULO 15. Política de seguridad digital para Teletrabajo y/o trabajo en casa. Las Direcciones	ARTÍCULO 15. Política de seguridad digital para Teletrabajo y/o trabajo en casa. Las Direcciones de Tecnología o quien haga sus veces en las entidades Sector Defensa, garantizarán la seguridad y óptimo funcionamiento de infraestructura tecnológica asignada a los servidores públicos, contratistas y terceros que laboren o realicen sus funciones en modalidad Teletrabajo o trabajo en casa, para lo cual deberán implementar las siguientes medidas:

			• Implementar controles en: Sistema de autenticación, código de desbloqueo o una clave para el acceso al mismo, uso de software de antivirus suministrado por la Entidad, restricción de privilegios administrativos para los usuarios y uso de software licenciado suministrado por la Entidad.	
			• Suministrar una conexión VPN segura - Virtual Private Network (Red privada virtual) para así prevenir la interceptación de posibles atacantes en la conexión. Esta conexión debe ser registrada y auditada por las Direcciones de Tecnología o quien haga sus veces en las entidades Sector Defensa.	
			• Para mitigar riesgos de seguridad de la información, emplear mecanismos para la autenticación y segregar funciones y responsabilidades de los usuarios con privilegios de administrador o que brindan soporte remoto.	
			• Realizar campañas de sensibilización sobre las políticas y controles de seguridad de la información para los servidores públicos, contratistas o terceros que apliquen al Teletrabajo o trabajo en casa.	
			• Realizar monitoreo y control permanente a la infraestructura que utilicen los trabajadores remotos en casa, con el fin de analizar posibles acciones no autorizadas.	
			PARÁGRAFO. La modalidad de Teletrabajo y/o trabajo en casa deberá estar implementada acorde a la normatividad referenciada en los considerandos de la presente resolución y deberá estar autorizada y reglamentada por la Dependencia que corresponda en la Entidad.	
		ARTÍCULO 16. Política de Certificados Digitales y Criptografía.	**ARTÍCULO 16. Política de Certificados Digitales y Criptografía**. La Direcciones de Tecnologías o quien haga sus veces en las entidades Sector Defensa, brindará a solicitud, herramientas que permitan el cifrado para proteger la confidencialidad, integridad, y disponibilidad de la información, transferencia a través de correo electrónico y otros mecanismos de transferencia de información a nivel interno y externo, así mismo:	

			a. Certificados Digitales. Deben implementar los mecanismos para incluir en los sitios web de la entidad certificados de servidor seguro SSL y la gestión para la revocación y renovación de los mismos. • Para mayor seguridad se requiere que los certificados SSL sean de tipo Extended Validation o lo que llaman en el mercado barra verde. • Se requiere escaneo automático periódico semanal en búsqueda de vulnerabilidades y escaneo automático diario de malware para detección de códigos maliciosos en el sitio asegurado. • Deben comprobar la existencia de la entidad físicamente, la propiedad del nombre del dominio, y la autoridad para solicitar el certificado. Deben cumplir con las características del formato estándar X.509 y acorde al RFC3280. • Deben tener compatibilidad con servidores de aplicaciones como IIS (Internet Information Server), OAS (Oracle Application Server), Oracle WebLogic, y demás que tenga la entidad. • Compatibilidad con algoritmos de cifrado RSA y ECC con la posibilidad de generar un certificado SSL para la misma URL por cada algoritmo de cifrado con el fin de garantizar la compatibilidad de todos los navegadores web. • Deben tener compatibilidad universal con navegadores y dispositivos móviles más comunes. • Compatibilidad con Subject Alternative Names (SAN) según sea requerido (esto hay que pedirlo en los contratos según lo que se vaya a asegurar). • Compatibilidad con ION o Nombres de Dominio Internacionalizado (dado posible cambio de DNS) • El tamaño del par de llaves (privada y pública) debe ser mínimo 2048bits, exigible 4096 cuando se declare inseguro el anterior.	

			b. Certificados de firma digital para servidores públicos: • Los certificados para uso de los servidores públicos deben ser de Función Pública. • Los certificados de firma digital deben ser emitidos por una Entidad de Certificación digital abierta acreditada por la ONAC {Organismo Nacional de Acreditación de Colombia) para la emisión de ese tipo de certificados digitales. • Los Certificados Firma digital Función Pública deben contener los datos mínimos requeridos en el artículo 35 de la Ley 527 de 1999 para su emisión, como son: • Nombre, identificación, dirección, teléfono correo electrónico del suscriptor. • Nombre de la Entidad y NIT donde realiza actividades el suscriptor. • El número de serie, fecha de emisión y fecha de expiración del certificado. • Adicional al cumplimiento normativo colombiano prescrito en la Ley 527 de 1999, Decreto Ley 0019 de 2012, el numeral 2 del artículo 15 del Decreto 333 de 2014, el Decreto 1471 de 2014, se debe requerir a la entidad de certificación el cumplimiento mínimo del estándar ITU X-509 V3 o superior y algoritmo de firma SHA256 o superior, exigible 4096 cuando se declare inseguro RSA 2048 bit, y de los Criterios Específicos de Acreditación para las Entidades de Certificación Digital CEA-4.1-10 Versión 01 y los reglamentos que los modifiquen, complementen o adicionen. • La prueba de posesión de la llave privada y solicitud de firma del certificado deben enviarse en formato PKCS#l0. • Debe soportar como mínimo los formatos de firma PADES, PADES LTV, XADES y CADES en formato CMS/PKCS#7 y PKCS#ll. • La Entidad de certificación Digital deberá mantener publicados y en línea los servicios CRL y OCSP oservicio web 7x24x365, 99.6% uptime por año, así como los certificados raíz y subordinado.	

			c. Gestión de llaves criptográficas: Se deben implementar las siguientes medidas: • El administrador del sistema o quien haga sus veces, será la persona responsable y encargada de la activación, recepción y la distribución de las llaves criptográficas a los usuarios autorizados y velará porque la llave se encuentre activa en el periodo de tiempo previsto. • Los responsables de las llaves criptográficas deberán almacenar las llaves de forma segura y se comprometerán a restringir el acceso sólo a los usuarios autorizados. De igual forma, una copia de las llaves (si esta existe) deberá ser almacenada en sitio seguro para su recuperación en caso tal que esta se extravíe. • El cambio o actualización de las llaves deberá ser solicitado por el personal responsable o quien haga su uso. •Las llaves serán revocadas por el responsable de seguridad de la información o persona delegada, cuando exista sospecha de que pudieron ser accedidas por una persona no autorizada o cuando el servidor público finalice su relación laboral con la Entidad. • La revocación y reposición de un Certificado de Firma Digital de Función Pública se da por cualquiera de los siguientes motivos: a. Pérdida del número de identificación personal (PIN) de acceso al certificado digital. b. Por muerte o incapacidad sobrevenida del suscriptor. c. Compromiso de la llave privada. d. Bloqueo del certificado digital. e. Por orden judicial o entidad administrativa competente. • Para todas y cada una de las actividades pertenecientes a la administración, gestión y eliminación de las llaves criptográficas, se deberá mantener registro de las actividades realizadas.	

		ARTICULO 17. Política de respaldo de Información.	ARTICULO 17. Política de respaldo de Información. La Direcciones de Tecnología o quien haga sus veces en las entidades del Sector Defensa, adoptarán medidas necesarias para asegurar el respaldo, custodia y recuperación de la información; para lo cual deberán:	
			• Asegurar que la información catalogada con cierto nivel de clasificación y reserva sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, retención, integridad y disponibilidad, según lo definido en el procedimiento Gestión de Copias de Respaldo de la entidad.	
			• Emitir y aprobar políticas y procedimientos de copias de respaldo de la información que mitiguen el riesgo de pérdida de información haciendo énfasis en sistemas de información que soporten los procesos misionales y críticos, teniendo en cuenta que las copias de seguridad se realicen tanto de los datos como de las configuraciones y se mantengan fuera de línea y soporten adecuadamente los planes de continuidad asociados a la operación de la entidad, definiendo con los responsables de la información los periodos de retención y custodia de dicha información.	
			• Almacenar los medios de copias de respaldo tanto localmente como en un sitio de custodia externa, garantizando en ambos casos la presencia de mecanismos de protección ambiental como detección de humo, fuego, humedad, así como mecanismos de control de acceso físico.	
			• Definir un plan de restauración de copias de respaldo que serán probados a intervalos regulares de tiempo, establecidos según las necesidades y capacidades de cada una de las entidades del Sector, con el fin de asegurar que son confiables en caso de emergencia.	
			• Disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos	

		ARTICULO 18. Política de transferencia de Información.	**ARTICULO 18. Política de transferencia de Información.** Las Direcciones de Tecnología o quien haga sus veces en las entidades del Sector Defensa, adoptarán medidas necesarias para asegurar la transferencia y seguridad de la Información, incluyendo la contenida en los mensajes electrónicos:	
			• Estableciendo convenios de trasferencia de información, en la que se incluya acuerdos de confidencialidad y acuerdos de protección de datos sobre el manejo de la información definiendo claramente la información a transferir que se realicen entre Entidades ya sea del Sector Defensa o externa	
			• Adoptando las medidas necesarias para la protección de mensajes contra acceso no autorizado, modificación o denegación del servicio, garantizando la confiabilidad y disponibilidad del servicio.	
			• Garantizando la coordinación y el intercambio de información con las autoridades competentes para facilitar los procesos de investigación ante amenazas cibernéticas, así como los que se requieran para soportar la contención, erradicación, recuperación y buenas prácticas ante incidentes de seguridad digital y ciberseguridad.	
		ARTÍCULO 19. Política General de la estrategia de Seguridad Digital	Las Direcciones de Tecnologías o quien haga sus veces en las entidades del Sector Defensa, a través de la dependencia de seguridad digital o similar, deberán implementar el Modelo de Seguridad y Privacidad de la Información (MSPI) en sus entidades y estar debidamente articulado con el habilitador de seguridad y privacidad de la política de Gobierno Digital, de acuerdo a los lineamientos emitidos en la Resolución 500 del 10 de marzo de 2021, expedida por MinTIC y demás normas que las desarrollan, adicionen o modifiquen. Adicionalmente, la estrategia de la Política de seguridad digital debe:	
			• Integrarse al Plan de Acción institucional.	
			• Ser aprobada a través de un acto administrativo por el Comité Institucional de Gestión y Desempeño o quien haga sus veces.	
			• Contar con un análisis y tratamiento de riesgos de seguridad digital y ciberseguridad e implementar controles que permitan emitir el Plan de Tratamiento de riesgos de la Entidad y como gestionarlos, teniendo en cuenta el	

			artículo 20 del presente documento. Así mismo coordinar con el área encargada la gestión de riesgos de ciberseguridad.
			• Establecer los roles y responsabilidades al interior de la entidad asociados a la seguridad digital y ciberseguridad.
			• Establecer e implementar los principios, lineamientos y estrategias para promover una cultura para la seguridad de la información, seguridad digital y ciberseguridad que incluya actividades de difusión, sensibilización y concientización para servidores públicos, contratistas y terceros para mejorar habilidades y promover conciencia en la seguridad de la información.
			• Incluir todas las tecnologías de la información y las comunicaciones que utiliza la organización, incluida la adopción de nuevas tecnologías o tecnologías emergentes.
			• Establecer los mecanismos de control (técnicos, tecnológicos y culturales) al interior de la entidad que permitan verificar el cumplimiento de las disposiciones establecidas en la política de seguridad de la información que hayan aprobado internamente, así como las medidas sancionatorias al incumplimiento de la misma a través de las Oficinas de Control Interno disciplinario o quien haga sus veces, realizando auditorias de seguridad de la información al menos una vez al año, que contemplen aspectos técnicos de la seguridad digital y ciberseguridad como análisis de vulnerabilidades a sistemas de información críticos, entre otros.
			• Incluir los elementos de valoración que se requerirán para determinar la conveniencia de contar con garantías que cubran los costos asociados a ataques cibernéticos.
		ARTÍCULO 20. Política para la gestión de riesgos de la seguridad de la información, seguridad digital y ciberseguridad.	La Dirección de Tecnología o quien haga sus veces en las entidades del Sector Defensa, a través de la dependencia de seguridad digital, unidades cibernéticas (en lo relativo a ciberseguridad) o similares, debe implementar los planes y controles para mitigar los riesgos que pudieran afectar la seguridad digital y física de acuerdo con el resultado de análisis y evaluación de riesgos y cumplir con las siguientes características y responsabilidades:

			Los planes de tratamiento de riesgos y los indicadores de eficacia o efectividad se deberán generar como lo indica el "esquema 9. Consolidación de los Planes y Tratamiento de Riesgos", de la "Guía para la administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles Entidades Públicas (Ver 5 - 2020)" emitidas por el DAFP y demás normas que las desarrollan, adicionen o modifiquen.	
			• Definir controles, considerando aspectos como estructura, tamaño, canales de atención, volumen transaccional, número de usuarios, evaluación del riesgo y servicios prestados por la entidad.	
			• Reportar los resultados del análisis de riesgos y gestión de incidentes, al comité institucional de gestión de desempeño o quien haga sus veces.	
			• Estar al tanto de las nuevas modalidades de ciberataques que pudieran llegar a afectar la entidad, según las políticas que establezca la misma, de acuerdo con su evaluación de riesgo y atendiendo criterios de razonabilidad.	
			• Asesorar a la alta dirección de la entidad sobre riesgos de seguridad de la infomiación, seguridad digital y ciberseguridad para que pueda hacer seguimiento y tomar las decisiones adecuadas en esta materia.	
			• Realizar un análisis de vulnerabilidades para determinar la pertinencia de contratar o implementar el servicio de un equipo especializado para atender incidentes de seguridad de la información, seguridad digital y ciberseguridad. El análisis debe identificar las características del proveedor, herramientas, servicios y privacidad de la información, entre otros.	
			• Cumplir los lineamientos de gestión del riesgo establecidos en la guía para la administración del riesgo y el diseño de controles en entidades públicas expedida en el marco del modelo integrado de planeación y gestión.	
			• Incluir en la estrategia de seguridad digital y en el plan de seguridad y privacidad de la información las medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas y controles para la gestión de los riesgos de seguridad y privacidad de la información por parte de funcionarios públicos, contratistas y terceros.	

		ARTÍCULO 21. Política de tratamiento para gestión de Incidentes de Seguridad Digital	La Oficina de Respuesta a Incidentes Cibernéticos-CSIRT, Unidades Cibernéticas o quien haga sus veces en las entidades del Sector, gestionarán los incidentes de seguridad digital y ciberseguridad y coordinaran las tareas de seguridad informática con quien correspondan si es del caso, para lo cual deberán:	
			• Formular e implementar el Plan Estratégico Institucional en materia de capacidades en Ciberseguridad y Ciberdefensa del Sector Defensa, hacer seguimiento, medición, análisis y evaluación.	
			• Las entidades del Sector Defensa deberán coordinar las capacidades de ciberseguridad con el CSIRT del Ministerio de Defensa Nacional y/o Comando Conjunto Cibernético - CCOCI del y ciberdefensa Comando General de las Fuerzas Militares y/o con el Centro Cibernético Policial - CCP de la Policía Nacional.	
			• Implementar las políticas de ciberseguridad y ciberdefensa de la infraestructura crítica en la Entidad de acuerdo con los lineamientos emitidos por el Ministerio de Defensa Nacional o las que emita el Gobierno a Nivel Nacional.	
			• Generar e implementar los protocolos, lineamientos, guías, estándares, buenas prácticas y recomendaciones de ciberseguridad y ciberdefensa para la entidad y hacer su seguimiento, medición, análisis y evaluación.	
			• Definir acciones, servicios de prevención, concientización y sensibilización ante amenazas cibernéticas y dar respuesta frente a incidentes en esta materia en la entidad.	
			• Cooperar con los organismos de seguridad e investigación del Estado en la prevención e investigación de delitos donde medien las tecnologías de la información y las comunicaciones.	
			• Formular e implementar planes, programas, proyectos y acciones que permitan generar y producir conocimiento relativo a la ciberseguridad y ciberdefensa para la entidad.	
			• Generar cultura en la entidad para crear, conservar, compartir, difundir, reconocer y valorar el conocimiento relativo a la ciberseguridad y ciberdefensa y	

			utilizar herramientas para su apropiación, seguimiento, medición, análisis y evaluación.	
			• Las entidades del Sector Defensa deberán coordinar y actuar como punto de contacto con el CSIRT del MDN y ColCERT.	
			• Gestionar y establecer mecanismos de prevención y control a los incidentes cibernéticos que puedan ocurrir en la entidad.	
			• Promover en la entidad el reporte obligatorio de incidentes cibernéticos, ofreciendo garantías de confidencialidad, privacidad, y beneficios de los mismos.	
			• Informar a los miembros del ecosistema cibernético del Sector Defensa acerca de las nuevas vulnerabilidades, advertencias y descubrimientos que afecten la seguridad cibernética.	
			• Coordinar con el CSIRT del MDN y ColCERT, la respuesta a incidentes cibernéticos de seguridad y defensa e implementar la infraestructura necesaria y hacer seguimiento a la gestión relacionada con el riesgo en estas materias.	
			• Incluir en su estrategia de seguridad digital como mínimo las actividades de prevención, protección y detección, respuesta y comunicación, recuperación y aprendizaje, según la resolución No.500 de marzo 10 de 2021 de MinTIC y las emitidas por el Gobierno Nacional; así como el Decreto 338 del 8 de Marzo de 2022 para fortalecer la gobernanza, las instancias y el modelo de atención y gestión y respuesta de incidentes de infraestructuras críticas cibernéticas y servicios esenciales.	
			• Disponer de un punto de contacto y un buzón de correo electrónico para facilitar el intercambio de información y gestión de incidentes de seguridad digital con el CSIRT del MDN y el ColCERT.	
			• Realizar los respectivos planes de mejoramiento, para lo cual el responsable de seguridad digital de la entidad supervisará y hará seguimiento a su cumplimiento.	

			• Promover entre los servidores públicos, contratistas y terceros, el reporte de manera inmediata y a través de los canales establecidos, de cualquier sospecha u ocurrencia de eventos considerados incidentes de seguridad de la información.	
			• Designar los responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, de acuerdo con su criticidad e impacto.	
			• Adelantar campañas de sensibilización y capacitación a los servidores públicos de la entidad, en ciberseguridad y ciberdefensa, y desarrollar procesos de formación especializada para las áreas a cargo de la ciberseguridad y ciberdefensa.	
			PARÁGRAFO. El CSIRT del Ministerio de Defensa tendrá a cargo la formulación, divulgación, implementación, seguimiento, medición, análisis y evaluación del Plan estratégico Sectorial en materia de capacidades en Ciberseguridad y Ciberdefensa del Sector Defensa; y de las políticas de ciberseguridad y ciberdefensa de la infraestructura critica del Sector Defensa, con la cooperación de los organismos de segurida del Sector.	
		ARTÍCULO 22. Enunciado de Política de Continuidad de la Operación.	La Dirección de Tecnología o quien haga sus veces en las entidades sector Defensa, será la encargada de la operación y administración de los recursos tecnológicos que soportan la operación, de definir e implementar el plan de continuidad tecnológico del negocio, así como los procedimientos de continuidad y de contingencia para cada una de las plataformas tecnológicas críticas bajo su responsabindad y cualquier estrategia orientado a generar el diagnóstico inicial, la contención, la respuesta, recuperación, reanudacipn _de la operación en contingencia y restauración ante la materialización de riesgos de seguridad de la información, seguridad digital y ciberseguridad, de tal forma que:	
			• Garantice la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad y disponibilidad de la información.	
			• Asegure que los cambios efectuados sobre los recursos tecnológicos sean autorizados y debidamente controlados.	

			• Provea la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo con el crecimiento de la Entidad. Adicionalmente deberán:	
			• Realizar ejercicios que permitan probar y garantizar la efectividad del plan de continuidad tecnológico del negocio frente al escenario de materialización de riesgos de seguridad de la información.	
			• Hacer una evaluación del nivel de madurez en Seguridad de Información, seguridad digital y ciberseguridad a través del instrumento de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información emitido por el MinTIC.	
			• Establecer, documentar y dar mantenimiento a los procedimientos de seguridad de la información que apliquen para la plataforma de tecnologías de información bajo su administración. PARÁGRAFO. La Oficina de Planeación o quien haga sus veces o quien designe la Alta Dirección en las entidades Sector Defensa, será la encargada de liderar el Plan de Continuidad del negocio de la entidad. Por otra parte, la Dirección de tecnología de la entidad o quien haga sus veces elaborará el análisis de impacto del negocio (BIA) y el Plan de continuidad tecnológico de la entidad.	
	CAPÍTULO III RESPONSABILIDADES DE LOS SERVIDORES PUBLICOS, CONTRATISTAS O TERCEROS FRENTE AL USO DE LOS RECURSOS TECNOLÓGICOS	**ARTÍCULO 23. Disposiciones**	Todos los servidores públicos, contratistas o terceros que hagan uso de los recursos tecnológicos de las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa tienen la responsabilidad de cumplir cabalmente las políticas establecidas para su uso aceptable, entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación y por ende, el cumplimento de la misión institucional.	
			a. Del uso de los recursos tecnológicos: los recursos tecnológicos de entidades del Sector Defensa son herramientas de apoyo a las labores y responsabilidades de los servidores públicos y contratistas. Por ello, su uso está sujeto a las siguientes directrices:	

			• Los bienes de cómputo no pueden ser utilizados con fines personales, estos se emplearán de manera exclusiva y bajo la completa responsabilidad del servidor público o contratista al cual han sido asignados, únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas.	
			• La Dirección de Tecnología o quien haga sus veces, deberá establecer y aplicar controles respecto al uso adecuado de los activos de información, así como la verificación de cumplimiento del software base y de aplicaciones, para prevenir la descarga, instalación y uso de software no licenciado y/o no autorizado, definiendo, manteniendo y controlando la lista de software y aplicaciones autorizadas para ser instaladas en las estaciones de trabajo de los usuarios, cumpliendo los criterios de autenticidad, vigencia, términos y condiciones legales para la utilización de la licencia.	
			• La Dirección de Tecnología o quien haga sus veces, deberá implementar mecanismos de gestión y monitoreo permanente a la infraestructura de TI de los servicios utilizados, incluyendo los de acceso remoto, con el fin de protegerlas de amenazas físicas y digitales.	
			• En caso de que el servidor público, contratista y/o terceros deba hacer uso de equipos ajenos a la entidad del Sector Defensa, éstos deberán cumplir con la legalidad del Software instalado, antivirus licenciado, actualizado y solo podrá conectarse a la red institucional, si es autorizado por la Dirección de Tecnologías o quien haga sus veces.	
			• Es responsabilidad de los servidores públicos, contratistas y terceros mantener copias de seguridad de la información contenida en sus estaciones de trabajo y entregarlas al finalizar la vinculación con la Entidad para su custodia.	
			• Está expresamente prohibido el almacenamiento en los discos duros de computadores de escritorio, portátiles o discos virtuales de red, de archivos de video, música y fotos que no sean de carácter institucional o que atenten contra los derechos de autor o propiedad intelectual de los mismos.	
			• No está permitido ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos o información física que pueda estar expuesta a daño parcial o total y, por ende, a la pérdida de la integridad de ésta.	

			• No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro eléctrico a los equipos de cómputo, salvo en aquellos casos autorizados expresamente por la dependencia responsable.	
			• Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, son las designadas para tal labor por la Dirección de Tecnología o quien haga sus veces.	
			• La Dirección de Tecnología o quien haga sus veces realizará monitoreo sobre los dispositivos de almacenamiento externos como USB, CD-ROM, DVD, Discos Duros externos, entre otros, con el fin de prevenir o detectar fuga de información.	
			• La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es la que tenga bajo su responsabilidad dicha función previa coordinación con la Dirección de Tecnología o quien haga sus veces, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de la gestión de bienes de la respectiva entidad Sector Defensa.	
			• La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, deberá ser informada de inmediato a la Dirección de Tecnología o quien haga sus veces por el servidor público, contratista o tercero a quien se le hubiere asignado; así mismo, deberá reponerse a la entidad o aplicar los procedimientos establecidos para este tipo de siniestros que estime la entidad.	
			• La pérdida de información deberá ser informada con detalle a la Dirección de Tecnología o quien haga sus veces, a través de la Mesa de Servicios o de ayuda, como incidente de seguridad.	
			• Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información física o digital deberá ser reportado a la mayor brevedad a la Dirección de Tecnología o quien haga sus veces, a través de la mesa de Servicios, siguiendo el procedimiento establecido.	
			• La Dirección de Tecnología o quien haga sus veces es la dependencia autorizada para la administración del software o para autorizar su	

			administración a otra dependencia, la cual no deberá ser copiado, suministrado a terceros ni utilizado para fines personales.	
			• Todo acceso a la red institucional deberá ser informado, autorizado y controlado por la Dirección de Tecnología o quien haga sus veces.	
			• La conexión a la red WiFi institucional para servidores públicos y contratistas deberá ser administrada desde la Dirección de Tecnología o quien haga sus veces, mediante un SSID (Service Set ldentifier) único; la autenticación deberá ser con usuario y contraseña de directorio activo u otro tipo de autenticación cuando aplique para la Entidad.	
			• La conexión a la red WiFi institucional para visitantes deberá tener un SSID y las contraseñas serán administradas por la Dirección de Tecnología o quien haga sus veces y las contraseñas deberán cambiar para el servicio de internet y estará restringida para la conexión a servicios institucionales.	
			• La red WiFi par a servidores públicos y contratistas estará disponible para sus equipos personales, teniendo en cuenta las capacidades técnicas, contractuales y lineamientos de seguridad establecidos por el Ministerio.	
			• Las redes inalámbricas (WiFi) de servicio en las entidades, deben ser redes para acceso y consulta de internet y no para que por medio de estas se administren infraestructuras internas o se acceda a servicios misionales internos desde dispositivos no corporativos, se exceptúan los casos autorizados por la Dirección de Tecnología o quien haga sus veces a funcionarios que cuenten con el perfil de administradores y se encuentre realizando actividades de trabajo remoto.	
			• Los equipos deben quedar apagados cada vez que el servidor público, contratista o tercero no se encuentre en la oficina o durante la noche; esto, con el fin de proteger la seguridad y distribuir bien los recursos de las entidades Sector Defensa; se exceptúa aquellos casos en que se esté realizando trabajo remoto.	

			• Cuando se utilicen aplicaciones de mensajería instantánea para actividades institucionales, deberán adoptarse políticas de seguridad y términos de uso de las aplicaciones, evaluando previamente los riesgos de vulnerabilidades de afectación a la confidencialidad, integridad y disponibilidad de la información.	
			• Los servicios de Tecnologías en la Nube deben aplicar las medidas de seguridad necesarias para garantizar la integridad, disponibilidad y confidencialidad de la información de la institución, así como cumplir con los requisitos establecidos en la normatividad vigente y con los niveles de seguridad adecuados para los servicios que presta cada entidad del Sector Defensa .	
			• Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y seguridad informática incluyendo los servicios en la nube de cada entidad del Sector Defensa, deberán estar protegidos mediante herramientas y software de seguridad que prevenga el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar posibles fallos.	
			• Cada entidad del Sector Defensa será responsable de que sus usuarios se mantengan actualizados acerca de los riesgos de infección de código malicioso provenientes de correos electrónicos, páginas Web, el intercambio de archivos o cualquier otra actividad de su operación diaria que pueda ser aprovechada por una amenaza.	
			• Todo dispositivo móvil personal que requiera acceder a los servicios tecnológicos de la entidad y que transmita y/o almacene información sensible debe ser monitoreado a través de la herramienta tecnológica definida por la Dirección de Tecnología o quien haga sus veces.	
			b. Del uso de dispositivos Institucionales de computación móvil como equipos portátiles, teléfonos móviles, tabletas, ef'!tre otros: la Dirección de Tecnología o quien haga sus veces en las entidades del Sector Defensa propenderá por el correcto uso, manejo y control de riesgos de seguridad de los dispositivos Institucionales de computación móvil como herramienta de trabajo asignada a los servidores públicos, contratistas o terceros, para facilitar las comunicaciones, cuando así se estime pertinente; para lo cual deberá:	

			• Verificar que los dispositivos móviles cuenten con los siguientes controles: Sistema de autenticación, como un patrón, código de desbloqueo o una clave para el acceso al mismo, uso de software de antivirus suministrado por la Entidad, restricción de privilegios administrativos para los usuarios y uso de software licenciado suministrado por la Entidad.	
			• Asegurar la conexión de los dispositivos móviles a la infraestructura tecnológica institucional, estableciendo los mecanismos de control necesarios para proteger la infraestructura tecnológica institucional	
			• Implementar técnicas criptográficas para cifrar la información crítica almacenada en los dispositivos de computación móvil.	
			• Mantener actualizados los sistemas operativos, navegadores, manejador de contenidos, librerías y, en general, todo el software, con las respectivas actualizaciones de seguridad liberadas por los fabricantes.	
			PARÁGRAFO 1. Los servidores públicos que pertenezcan a las entidades del Sector Defensa, deben cumplir con las siguientes responsabilidades frente al correcto uso de los dispositivos Institucionales de computación móvil:	
			• Los teléfonos móviles y/o teléfonos inteligentes institucionales, debe permanecer encendidos y cargados como mínimo durante las horas laborales	
			• El uso del dispositivo móvil suministrado debe ser para realizar actividades propias de su cargo o funciones asignadas en la entidad.	
			• No están autorizados a cambiar la configuración, ni a la desinstalación de software de los equipos móviles institucionales posterior a su recibo; únicamente se deben aceptar y aplicar las actualizaciones.	
			• Evitar hacer uso de los dispositivos móviles en lugares con algún riesgo de seguridad, con el fin de evitar el extravío o hurto del equipo.	
			• No se debe hacer uso de los dispositivos móviles en redes inalámbricas públicas.	

			PARÁGRAFO 2. El servidor público, contratista o tercero que por necesidades del servicio requiera hacer uso de los servicios tecnológicos de la entidad en sus dispositivos personales deberá contar con la autorización del Director de la dependencia o similar. Así mismo aceptar términos y condiciones y permitir la instalación de la herramienta de control que la Dirección de Tecnología o quien haga sus veces tiene para este fin.	
			c. Del uso del correo electrónico institucional.	
			• El único servicio de correo electrónico autorizado para el manejo o transmisión de la información Institucional en la Entidad es el asignado por la Dirección de Tecnología o quien haga sus veces, con el dominio @entidad.gov.co o @entidad.mil.cao el dominio de la entidad, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando cualquier tipo de ataque cibernético. Así mismo deberán contener una sentencia de confidencialidad, que será diseñada por La Dirección de Tecnología, con el apoyo de la Oficina de Comunicaciones Estratégicas y la oficina Jurídica, o similares en la entidad.	
			• El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional y debe contener cuando aplique la firma digital de la entidad por medio de un método criptográfico; en consecuencia, no puede ser utilizado con fines personales, económicos, comerciales o cualquier otro fin ajeno a los propósitos de la Entidad.	
			• La Dirección de Tecnología o quien haga sus veces en la entidad, implementará herramientas tecnológicas que prevengan la pérdida o fuga de información de carácter reservado o clasificado, de conformidad con las leyes estatutarias 1266 de 2008, 1581 de 2012, 1621 de 2013 y 1712 de 2014.	
			• Se permite el envío masivo de correos de carácter institucional desde cuentas corporativas, los cuales deben cumplir con las características de comunicación e imagen corporativa y ser asignadas a un responsable para garantizar el correcto uso de estas.	

			• Para facilitar la gestión de correo electrónico de directivos, el titular debe solicitar a la respectiva mesa de servicios la delegación del buzón correspondiente, relacionando los colaboradores que podrán escribir o responder en nombre del titular, con el fin de mitigar la suplantación.	
			• Todo mensaje SPAM, cadena, de remitente o contenido sospechoso, debe ser inmediatamente reportado a la Dirección de Tecnología o quien haga sus veces, a través de la respectiva Mesa de Servicios o similar, como incidente de seguridad según el procedimiento establecido, y deberán acatarse las indicaciones recibidas para su tratamiento.	
			• La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, o cualquier otra ajena a los fines de la entidad.	
			• Está expresamente prohibido el uso del correo institucional para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y que atenten contra la integridad moral y/o buena imagen de las personas o instituciones.	
			• El cifrado de los mensajes será necesario siempre que la información transmitida desde un correo electrónico institucional esté catalogada como clasificada o reservada en el inventario de activos de información o en el marco de la Ley Colombiana vigente.	
			La Dirección de Tecnología o quien haga sus veces, deben coordinar internamente la identificación de los buzones de correo institucionales que se considere su contenido como información relevante para la Entidad y por ello se hace necesario salvaguardar la información de acuerdo con las regulaciones vigentes en cuanto a preservación y conservación documental establecidas por el Archivo General de la Nación y Ministerio de Tecnologías de la Información y Comunicaciones	

			Las entidades del Sector Defensa se reservan el derecho de monitorear los accesos y el uso de los buzones de correo institucional (@entidad.gov.co o@entidad.mil.co), de todos sus servidores públicos o contratistas. Además, podrá realizar copias de seguridad del correo electrónico institucional (@entidad.gov.co o @entidad.mil.co) en cualquier momento sin previo aviso y limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información propios o de terceros operados en las entidades Sector Defensa, previa solicitud expresa del Ministro de Defensa, Viceministros, Comandante General de las Fuerzas militares, Comandante de Fuerza, Director de la Policía Nacional, del nominador, ordenador del gasto, supervisor del contrato, jefe inmediato, Control Disciplinario Interno, Gestión del Talento Humano, La Dirección de Tecnología o quien haga sus veces.	
			d. Del uso de Internet: La Dirección de Tecnología o quien haga sus veces, a través del Jefe de Seguridad de la Información o quien haga sus veces, establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones y será responsabilidad de los colaboradores las siguientes, entre otras:	
			• Los servicios a los que un determinado usuario pueda acceder en internet dependerán del rol o funciones que desempeña en las entidades del Sector Defensa y para las cuales esté formal y expresamente autorizado por su jefe o supervisor, y solo se utilizará para fines laborales.	
			• No está permitido enviar, descargar y visualizar páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor o que atenten contra la integridad moral de las personas o de las instituciones.	
			• No está permitido enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida.	
			• No está permitido acceder a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas por la política de navegación de las entidades del Sector Defensa.	
			• No está permitido enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida.	

			• No está permitido propagar intencionalmente virus o cualquier tipo de código malicioso.	
			• Las entidades que de acuerdo con, su tamaño, despliegue de infraestructura tecnológica, superficie de exposición e internet y los servicios y sistemas esenciales críticos que gestionen, deben conformar un Equipo o Grupo de Seguridad Digital y nombrar el oficial de seguridad de la información, quien será el encargado de verificar la correcta aplicación de las políticas y estrategias vigentes en su entidad dentro encargado de verificar la correcta aplicación de las políticas y estrategias vigentes en su entidad dentro del marco del cumplimiento de las misión y funciones asignadas.	
			• Las entidades del Sector Defensa deben implementar protocolos y políticas de acceso remoto que impidan a los usuarios escalar privilegios y que mitigue el riesgo de acceso no autorizado a recursos o información.	
			• La Dirección de Tecnología o quienes haga sus veces se reservan el derecho de monitorear los accesos y el uso del servicio de Internet, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro uso ajeno a los fines institucionales	
			e. Del uso de las redes sociales: Todos los servidores públicos son responsables de la información que generan, acceden y procesan, así como de evitar su uso indebido, para lo cual se dictan los siguientes lineamientos:	
			• Las redes sociales de carácter institucional no deben ser abiertas a nombre propio de funcionarios o contratistas sino de la entidad.	
			• El funcionario responsable del manejo de las redes sociales institucionales debe garantizar el uso adecuado de las mismas.	
			• El uso de las redes sociales de carácter institucional debe ser controlada por la Dirección de comunicación de la entidad o similares, con el fin de contar con niveles de protección adecuados para un uso correcto y seguro de estas plataformas en apoyo con la Dirección de Tecnología o quien haga sus veces.	

			• Se deben utilizar soluciones de seguridad, configurar correctamente los usuarios en las redes sociales, utilizar cuando sea posible un segundo factor de autenticación y el protocolo HTTPS para la navegación, entre otros.
			• Se requiere no utilizar un usuario con permisos de administrador al momento de navegar en las redes sociales, y que cada funcionario permitido cuente con sus propios perfiles. Esta es una forma de minimizar el impacto en caso de que ocurra un incidente.
			• No utilizar la contraseña de una red social en otros sitios de internet y nunca compartirla, aplicar reglas de contraseña segura, evitar utilizar computadoras públicas para ingresar en las redes sociales institucionales.
			f. Del uso del escritorio, pantalla limpias y periféricos: Todos los servidores públicos, contratistas o terceros que laboran en las entidades del Sector Defensa y que hagan uso de estaciones de trabajo, deberán acatar las siguientes disposiciones:
			• En horas no hábiles, o cuando los sitios de trabajo se encuentren desatendidos, dejar los medios que contengan información crítica protegida bajo llave.
			• 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 lo bloqueó.
			•Tomarlas medidas de seguridad necesarias en el uso de sus contraseñas, para evitar que estas sean conocidas por personal interno o externo a la Entidad.
			• Cuando se imprima o digitalice documentos con información pública clasificada o pública reservada, éstos deben retirarse inmediatamente de dichos dispositivos.
			• Los dispositivos de impresión y digitalización deben permanecer limpios de documentos.
			• Los documentos que contengan información institucional sensible no deben ser reutilizados y destruirse de acuerdo con los parámetros y normatividad vigente establecida en la ley de Archivo General vigente.

			g. Del uso de los sistemas o herramientas de Información: Todos los servidores públicos, contratistas o terceros que laboran en las entidades del Sector Defensa son responsables de la protección de la información que acceden y procesan, así como de evitar su pérdida, alteración, destrucción y uso indebido, para lo cual se dictan los siguientes lineamientos:	
			• Las credenciales de acceso a la red y a los recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible.	
			• Es responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos asignados de acuerdo con las políticas de administración de usuarios establecidas en la entidad.	
			• Es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.	
			• Cuando se ausenta por vacaciones, permiso, comisiones, excusas médicas, entre otros, deberá solicitar a través de la mesa de servicios o similar, el bloqueo de acceso a la estación de trabajo y la cuenta de correo electrónico institucional, a la-Dirección de Tecnología o quien haga sus veces, así mismo si tienen asignado accesos a sistemas de información, deberá reportar a los entes correspondientes para que inactiven las respectivas licencias, con el fin de evitar la fuga de la información, el acceso a terceros, lo cual pueda generar daño, alteración o uso indebido a la información, así como la suplantación de identidad. Las dependencias de Gestión del Talento Humano o las que hagan sus veces, y supervisores de los contratos, deberán reportar inmediatamente cualquier tipo de novedad que presenten los servidores públicos, contratistas o terceros a la Dirección de Tecnología o quien haga sus veces. servidores públicos, contratistas o terceros a la Dirección de Tecnología o quien haga sus veces.	
			• Cuando cesa sus funciones o culmina la ejecución de contrato con la respectiva entidad del Sector Defensa, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente; la información del servidor público o contratista será almacenada en los repositorios establecidos por cada una de las Entidades del Sector Defensa de acuerdo a sus políticas de archivo y conservación de la información.	

			• Cuando cesa sus funciones o culmina la ejecución de contrato con la respectiva entidad, el jefe inmediato o supervisor es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual, de acuerdo con la normativa vigente.
			• Dar estricto cumplimiento a la reglamentación vigente sobre derechos de autor.
	CAPÍTULO IV MEDICIÓN, CUMPUMIENTO, REVISIÓN Y VIGENCIA	**ARTICULO 24. Medición**	La aplicación de indicadores de gestión al modelo de operación del marco de seguridad y privacidad de la información en las entidades Sector Defensa, están orientados principalmente en la medición de efectividad, eficacia y eficiencia de los componentes de implementación y gestión de los planes de seguridad digital, definidos en cada una de las entidades del Sector Defensa, para lo cual se recomienda aplicar la "Guía No 9 de indicadores de gestión de seguridad de la información' emitida por el MinTIC y el "esquema 9. Consolidación de los Planes y Tratamiento de Riesgos', de la "Guía para a la administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles Entidades Públicas (Ver 5 - 2020!' emitidas por el DAFP.
		ARTÍCULO 25. Cumplimiento.	Cumplimiento. La Alta Dirección de las entidades del Sector Defensa, verificarán el cumplimiento de la presente Resolución, en particular la definición de una estrategia que permita brindar servicios, controles y condiciones que garanticen la Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de las entidades.
			PARAGRAFO. Las oficinas o dependencias de Control Interno, durante la realización de las auditorías, validarán y consignarán en sus informes el nivel de cumplimiento de los lineamientos de la presente Resolución, así como de la aplicación de controles sobre los activos de información y los requerimientos del Modelo de Seguridad y Privacidad de la Información (MSPI) en las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa.

		ARTÍCULO 26. Revisión	La Dirección de Tecnologías de la Información y Comunicaciones -TICS del Ministerio de Defensa, revisará anualmente, o antes si existiesen modificaciones que así lo requieran, los lineamientos consignados en la presente resolución. Así mismo será revisado por el Comité del Modelo Integrado de Planeación y Gestión Sectorial o el que haga sus veces del Ministerio de Defensa Nacional.
		ARTÍCULO 27. Vigencia	Vigencia. La presente Resolución deroga la Directiva Ministerial DIR2014-18 "Políticas de Seguridad de la información para el sector Defensa', y rige a partir de la fecha de su publicación

REVISADO Y APROBADO

	ELABORADO	**REVISADO (Coordinador)**	**REVISADO (Planeación)**	**APROBADO (Director)**
Nombres y Apellidos Grado y Cargo Fecha				OCAMPO NAHAR GUSTAVO ADOLFO Firmado digitalmente por OCAMPO NAHAR GUSTAVO ADOLFO Fecha: 2025.06.09 21:48:07 -05'00'
	Yeny Aracelly Nuñez Rosero	CR(R) Andrea del Pilar Diaz Rodriguez	Paola M. Calderón Pérez	MG (R) Gustavo Adolfo Ocampo Nahar
	Profesional Defensa- TIC	Coordinadora Administrativa y Financiera	Asesor Defensa – Área de Planeación	Director de Veteranos y Rehabilitación Inclusiva
	29-05-2025	29-05-2025	29-05-2025	29-05-2025

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

02	modificación	Adopción de la resolución 7870-2022 Por la cual se emite y adopta la Política General de Seguridad y Privacidad de la información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios en las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa, y se dict.an otras disposiciones'.	29/05/2025	Paola M. Calderón Pérez