COMANDO GENERAL FUERZAS MILITARES

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PRODOPAC
AYUDANTIA GENERAL DE LAS FUERZAS MILITARES

BOGOTÁ, D.C. 2020

I. INTRODUCCIÓN

El Comando General de las Fuerzas Militares, mediante Resolución 047 del 03 de marzo del 2020, -"Por la cual se adopta el Modelo Integrado de planeación y Gestión en el Comando General de las Fuerzas Militares, se conforma el "Comité Institucional y Desempeño" se establece otros lineamientos y se deroga la Resolución No. 091 de 26 de mayo de 2014", en el artículo 4°. Planes. A partir del Plan Estratégico Militar PEM 2030, el Comando General de las Fuerzas Militares, *realiza el Plan de Acción institucional Anual, el cual contendrá las acciones relacionadas con las* Políticas de Gestión y Desempeño Institucional e incluirá en sus líneas de acción, (...) La implementación del MIPG, a través de sus dimensiones y eje articulador señalados en los artículos 2° y 3° de este acto administrativo, responden a los requisitos y lineamientos normativos, a la dinámica organizacional y a mecanismos que facilitan la articulación de modelos y sistemas como lo son el MIPG, Responsabilidad social institucional, modelo de seguridad y privacidad de la información, entro otros.(...), e indica los procesos relacionados con la alineación de las políticas del MIG, indicando que (...) La política de Gobierno digital (en donde se encuentra como habilitador el Modelo de Seguridad de la Información) los Procesos (Fortalecimiento organizacional, Gestión de TI, Direccionamiento estratégico, Gestión jurídica, Comunicación estratégica, Gestión de recursos administrativos) y la política de Seguridad digital (Fortalecimiento organizacional, Gestión de TI, Direccionamiento estratégico, Gestión jurídica)(...), así mismo, en el artículo 11° por el cual se establecen las responsabilidades del Comité MIPG,. Además, el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital, de igual manera el Decreto 2106 de 2019, Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública, en el parágrafo del artículo 16 indica que (...)Las autoridades deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.(...).

Teniendo en cuenta lo anterior, se crea el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018 "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", al interior del Comando General de las Fuerzas Militares, aprobado mediante acta de la sesión 0120006006902 de comité del Modelo Integrado de Planeación y Gestión – MIPG de fecha 11 de Agosto de 2020

II. REFERENCIAS

A. Constitución Política de Colombia
B. Ley 80 de 1993 "Por la cual se expide el Estatuto General de Contratación de la Administración Pública".
C. Ley 87 de 1993 "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones".

D. Ley 527 de 1999 "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".
E. Ley 594 de 2000 " Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones "
F. Ley 734 de 2002 "Por la cual se expide el Código Disciplinario Único"
G. Ley 1266 de 2008 "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".
H. Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
I. Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" y su decreto reglamentario 1377 del 27 de junio de 2013.
J. Ley 1621 de 2013 "Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones".
K. Ley 1712 de 2014 "Por medio del cual se crea la Ley de Transparencia y del Derecho al Acceso a la Información Púbica y se dictan otra disposiciones".
L. Ley 1862 de 2017 "Por la cual se establecen las normas de conducta del Militar Colombiano y se expide el Código Disciplinario Militar".
M. Ley 1955 del 2019 "Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad"
N. Decreto 103 de 2015 "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones"
O. Decreto 1080 de 2015 "Por medio del cual se expide el Decreto Reglamentario Único del Sector Cultura".
P. Decreto 1494 del 2015 "Por el cual se corrigen yerros en la Ley 1712 de 2014".
Q. Decreto 1074 de 2015. "por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo".
R. Decreto 1078 de 2015."Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
S. Decreto 1081 de 2015."Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia".
T. Decreto 728 de 2017."Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico"
U. Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

V. Decreto 1008 del 2018."Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".

W. Decreto 2106 de 2019."Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública".

X. Resolución 047 de 2020. Por la cual se actualiza el Modelo Integrado de Gestión (MIG) del Comando General de las Fuerzas Militares, se conforma el "Comité Institucional de Gestión y Desempeño" se establecen otros lineamientos y se deroga la Resolución 091 de 2014.

III. VIGENCIA.

Al presente plan rige a partir de la fecha de aprobación hasta el 31 de diciembre de 2021

IV. DEFINICIONES.

A. Las siguientes definiciones con el fin de fijar con claridad, exactitud y precisión sobre el tema.

1. Activo de información: Aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida. (Ley 1712 de 2014)
2. Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
3. Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y evaluar objetivamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
4. Autorización tratamiento de datos personales: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales. (Art 3. Ley 1581 de 2012).
5. Aviso de privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales. (Art 3. Decreto 1377 de 2013).
6. Base de datos: Conjunto organizado de datos personales que sea objeto de tratamiento debe distinguirse dos clases de bases de datos; las automatizadas, es decir, aquellas que se almacenan y administran a través de herramientas informáticas y las bases de datos manuales o archivos, donde la información se encuentra organizada o almacenada en medio físico y contienen información personal, tal como nombre, identificación, números de teléfono, correo electrónico. (Art 3. Ley 1581 de 2012).
7. Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, ssistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
8. Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales. La ciberseguridad tiene el fin de proteger a los usuarios y los activos de Estado en el Ciberespacio (CONPES 3995).
9. Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. (Decreto 1078 de 2015), (ISO27001).

10. Contratistas: Entenderemos por contratista aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con una entidad. (ISO/IEC 27002:2013).
11. Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.(ISO27001:2013).
12. Custodio de la Información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. (ISO/IEC 27002:2013).
13. Dato personal o información personal: Corresponde a cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Art. 3. Ley 1581 de 2012). Para efectos de la presente Directiva se entiende como la información suministrada por el usuario para su registro, lo cual incluye nombre, identificación, edad, género, dirección, correo electrónico y teléfono, entre otros. (Art. 3. Ley 1581 de 2012)
14. Dato privado: Es el dato que por su naturaleza intima o reservada, sólo es relevante para el titular. (Art 3. Ley 1266 de 2008).
15. Dato público: 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. (Art 3. Decreto 1377 de 2013).
16. Dato semiprivado: Es 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 dato financiero, y crediticio de actividad comercial o de servicios a que se refiere el título IV de la Ley 1266. (Art 3. Ley 1266 de 2008).
17. Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, etc. (Art 3. Decreto 1377 de 2013).
18. Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
19. Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. (Ley 1712 de 2014).
20. Dueño del riesgo sobre el activo: Persona responsable de gestionar el riesgo. (ISO/IEC 27001).
21. Encargado del tratamiento: 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. (Art 3. Ley 1581 de 2012).
22. Foro: Servicio automatizado de mensajes, a menudo moderado por un propietario, a través del cual los suscriptores reciben mensajes dejados por otros suscriptores por un tema dado. Los mensajes pueden ser enviados, entre otros, por correo electrónico.
23. 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. (ISO/IEC 27000).
24. Guía: Documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información. (ISO/IEC 27001).

25. Impacto: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo. (ISO/IEC 27001).
26. Incidente de seguridad de la información: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información. (ISO/IEC 27001).
27. Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en 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 circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ad 6. Ley 1712 de 2014).
28. 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.
29. Información Pública: Es toda información que un sujeto obligado genere, obtenga, adquiera o controle en su calidad de tal. (Art 6. Ley 1712 de 2014).
30. Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. (Art 6. Ley 1712 de 2014).
31. Oficial de Seguridad: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información. (Guía para la Gestión y Clasificación de Activos de Información GUIA 5 - MSIP-MINTIC).
32. Parte interesada (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.(ISO9001:2015).
33. PIGDP: Programa Integral de Gestión de Datos Personales; Resultado de un proceso de debida diligencia al interior de la organización que incorpora políticas que respondan a los ciclos internos de gestión de datos y que generen resultados medibles, mediante la aplicación de buenas prácticas de gestión de datos personales. (Ley 1581 de 2012).
34. 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).
35. 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).
36. Política del SGSI: Manifestación expresa de apoyo y compromiso de la alta dirección con respecto a la seguridad de la información. (ISO/IEC 27001).
37. Privacidad de datos: La privacidad de datos, también llamada protección de datos, es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad.(Ley 1581 de 2012).
38. Propietario de la Información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados. (Ley 1712 de 2014).
39. PSE: Proveedor de Servicios Electrónicos, es un sistema centralizado por medio del cual las empresas brindan a los usuarios la posibilidad de hacer sus pagos por Internet. (Ley 1340 de 2009).
40. Publicar: Hacer que un documento, o una información, determinados sea visible a través del sitio web institucional. (Estrategia de Gobierno Digital, MinTIC, Ley 1712 de 2014).
41. Registro Nacional de Bases de Datos (RNBD): Es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país. El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos (Art 25. Ley 1581 de 2012).

42. Responsable del tratamiento: 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. (Art 3. Ley 1581 de 2012).
43. Responsables del Activo: Personas responsables del activo de información.(ISO 27001:2013)
44. Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control. (NTC GTC137).
45. Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo. (ISO 27001:2013).
46. Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza. (ISO 27001:2013).
47. SARL: Siglas del Sistema de Administración de Riesgo de Liquidez. (ISO/IEC 27001:2013).
48. SARLAFT: Siglas del Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo. (ISO/IEC 27001:2013).
49. SARO: Siglas del Sistema de Administración de Riesgos Operativos. (ISO/IEC 27001:2013).
50. Seguridad de la información Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
51. SGSI: Siglas del Sistema de Gestión de Seguridad de la Información (ISO/IEC 27001:2013).
52. Sujetos Obligados: Se refiere a cualquier persona natural o jurídica, pública o privada incluida en el artículo 5 de la Ley 1712 de 2014.
53. Titular: Persona natural cuyos datos personales sean objeto de tratamiento. (Art 3. Ley 1581 de 2012).
54. Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país. (Art 3. Decreto 1377 de 2013).
55. Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia, cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable. (Art 3. Decreto 1377 de 2013).
56. Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales. Tales como la recolección, almacenamiento, uso, circulación o supresión. (Art 3. Ley 1581 de 2012).
57. 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).
58. Usuario: Es la persona natural o jurídica que, en los términos y circunstancias previstos en la ley 1266 de 2008, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. (Art 3. Ley 1266 de 2008).
59. Vulnerabilidad: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada.

V. OBJETIVO GENERAL

Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio, en el Mapa de Procesos del Comando General de las Fuerzas Militares

– COGFM, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información, enmarcado en el Sistema de Gestión de Seguridad de la información, con el fin proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información que circula en el mapa de procesos; mediante una gestión integral de riesgos y la implementación de controles físicos y digitales previniendo así incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así por el acceso, uso efectivo y apropiación masiva de las tecnologías de información y comunicación a través de políticas y programas.

A. OBJETIVOS ESPECIFICOS

1. Contribuir al incremento de la transparencia de la gestión pública.
2. Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información.
3. Dar lineamientos para la implementación de la gestión de seguridad y privacidad de la información.
4. Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de seguridad digital.
5. Contribuir a mejorar los procesos de intercambio de la información pública.
6. Orientar a la entidad en las mejores prácticas para la construcción de políticas de privacidad respetuosa de los datos personales de los titulares.
7. Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital y continuidad de la operación de manera integral.
8. Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.
9. Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la información del Comando General de las Fuerzas Militares.
10. Definir los lineamientos necesarios para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.
11. Generar conciencia para el cambio organizacional requerido para la apropiación de la Seguridad y Privacidad de la Información como eje transversal del Comando General de las Fuerzas Militares.
12. Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

VI. DESARROLLO DEL TEMA.

A. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Aplica a todos los niveles del Comando General de las Fuerzas Militares, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del Comando General de la Fuerzas Militares creen, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, sin importar el medio, formato, presentación o lugar en el cual se encuentre, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación.

OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI.

Gráfico N°. 1. **Sistema de Gestión de Seguridad y Privacidad de la Información – SGSI.**

B. POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

El Comando General de las Fuerzas Militares, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para el Comando General de las Fuerzas Militares, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con el objeto de mantener un nivel de exposición, que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, ésta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI, estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalece la cultura de seguridad de la información en los funcionarios, terceros, aprendices, participantes y clientes del Comando General de las fuerzas Militares.
- Garantizar la continuidad del negocio frente a incidentes.

El Comando General de las Fuerzas Militares ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros conforme a las necesidades de la entidad y a los requerimientos regulatorios, estableciendo para ello la identificación de normas de aplicabilidad en cada uno de los procesos del Comando General.

1. Gestión de Activos
2. Control de Accesos
3. Criptografía
4. Seguridad Física y del Entorno
5. Seguridad de las Comunicaciones
6. Seguridad de la Operaciones
7. Relaciones con los Proveedores
8. Adquisición, Desarrollo y Mantenimiento de Sistemas
9. Incidentes de Seguridad de la Información

C. PRINCIPIOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LAS INFORMACIÓN.

El incumplimiento a la política de seguridad y privacidad de la información del Comando General de las Fuerzas Militares, traerá consigo, las consecuencias legales que aplique a la normatividad vigente de orden Nacional e Internacional.

1. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas o terceros.
2. Protegerá su información institucional de las amenazas originadas por factores internos y externos que afecten cualquiera de sus principios.
3. Protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
4. Controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
5. Implementará control de acceso a la información, sistemas y recursos de red.
6. Garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
7. Garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
8. Garantizará la confiabilidad y el nivel de sensibilidad de la información que provenga de terceros y de sistemas de información con los cuales se tenga interoperabilidad.
9. Garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
10. Actualizará la política teniendo en cuenta la valoración de riesgos de procesos y de seguridad de la información.

D. ORGANIZACIÓN DE LAS SEGURIDAD DE LA INFORMACION

1. Responsable de la seguridad de la Información

El Comando General de las Fuerzas Militares dentro de su organización estructural cuenta con la Dirección de Tecnología de la Información, que será la responsable de la seguridad a nivel Estratégico en el Comando General y tendrá las siguientes responsabilidades:

a. Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo.
b. Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.
c. Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.
d. Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.
e. Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos.
f. Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo
g. Encarrilar el proyecto hacia el cumplimiento de la implementación del Modelo de Seguridad y privacidad de la Información para la entidad.
h. Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.
i. Monitorear el estado del proyecto en términos de calidad de los productos, tiempo y los costos.
j. Trabajar de manera integrada con el grupo o áreas asignadas.
k. Asegurar la calidad de los entregables y del proyecto en su totalidad.

2. Alcance y Aplicabilidad

Las capacidades establecidas en el presente plan y sus posteriores actualizaciones, tienen alcance y aplican a todos los recursos y activos de información del Comando General de las Fuerzas Militares, así como a los designados para su uso y custodia en el territorio nacional y fuera de él, en lo relacionado con la seguridad y privacidad de la información del Comando General de las Fuerzas Militares y sus Unidades Adscritas y Asociadas.

3. Nivel de Cumplimiento.

Todas las Personas Naturales como Jurídicas cubiertas por el alcance y aplicabilidad deberán cumplir el 100% en desarrollo y ejecución de la política.

Tabla de Responsabilidades – Marco Arquitectura Empresarial.

DOMINIO	RESPONSABILIDADES
SERVICIOS TECNOLÓGICOS	• Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución. • Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. • Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. • Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. • Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información
ESTRATEGIA TI	• Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información.
GOBIERNO TI	• Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI. Encargado monitorear y gestionar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información.
SISTEMAS DE INFORMACIÓN	• Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad. • Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano. • Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. • Liderar el proceso de gestión de incidentes de seguridad así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados. • Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio
DE INFORMACIÓN	• Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. • Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información.
USO Y APROPIACIÓN	• Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles. • Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora. • Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.

4. Conformación del Comité

Esta función estará bajo la responsabilidad del Departamento de Conjunto de Comunicaciones CGDJ6 el cual conformará el Subcomité de Seguridad de la Información que deberá asegurar que exista una Dirección y Apoyo Gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso adecuados, así como la formulación y mantenimiento de una política de seguridad de la información a través de la entidad.

E. ORGANICION DE LAS POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

1. Seguridad del Recurso Humano.

   Esta responsabilidad estará bajo el control y supervisión de la Dirección de Personal del Comando General de las Fuerzas Militares, será quien definirá los protocolos en la capacitación y sensibilización del personal en temas de seguridad de la información teniendo en cuenta las diferentes roles y responsabilidades entre otros como líder del proceso de Gestión del Talento Humano GETH-MIPG.

   a. Planeación: Que involucra momentos de direccionamiento estratégico, seguimiento y evaluación (Ingreso, Desarrollo y Retiro)
   b. Política de Integridad: La integridad es una característica personal, que en el sector público se refiere al cumplimiento de la promesa que cada servidor le hace al Estado y a la ciudadanía de ejercer a cabalidad su labor.
   c. En el procedimiento de ingresos y desvinculación del personal, gestionara de forma segura los protocolos y procedimientos al interior incluyendo temas de verificación de antecedentes, firmas de acuerdo de confidencialidad, recepción de entregable de los activos de la información, generación de paz y salvos.

2. Gestión de Activos

   Cada Jefatura, Subjefaturas, Departamento, Dirección, Sección, Unidades del Comando General de las Fuerzas Militares, tienen la custodia sobre todo dato, información y mensaje generado, procesado y contenido por sus sistemas de cómputo, así como también de todo aquello transmitido a través de su red de telecomunicaciones o cualquier otro medio de comunicación físico o electrónico y se reserva el derecho de conceder el acceso a la información. Por lo tanto deben:

   a. Clasificación de Activos:

LEY 1712 DE 2014		LEY 1621 DE 2013 DE INTELIGENCIA			
PÚBLICO CLASIFICADO	PÚBLICO RESERVADO	SECRETO	ULTRA SECRETO	CONFIDENCIAL	RESTRINGIDO

   Identificar los activos asociados a cada sistema de información, sus respectivos propietarios y su ubicación a fin de elaborar y mantener un inventario ac tualizado de los activos de información, de acuerdo al procedimiento de Inventario y Clasificación de Activos de Información emitido por el Departamento Conjunto de Comunicaciones CGDJ6 para los inventarios de Software, Hardware, Servicios y del proceso de gestión documental por la Dirección de Gestión Documental teniendo en cuenta la normatividad vigente.

   Realizar la clasificación y control de activos de información con el objetivo de garantizar que estos reciban un apropiado nivel de protección, clasificar la información para señalar su sensibilidad y criticidad y definir los niveles de protección y medidas de tratamiento de acuerdo al procedimiento de Inventario y Clasificación de Activos de Información,

evaluando las tres características de la información en las cuales se basa la seguridad de la información: confidencialidad, integridad y disponibilidad.

Gráfico N°. 2 Operación Sistema de Gestión de Seguridad y Privacidad de la Información – SGSI.

b. Clasificación de la Información.

Los líderes de los procesos propietarios de los activos de información, son los responsables de establecer el nivel de clasificación de cada activo, para asignar el carácter de clasificada o reservada a la información pública que se encuentra bajo su posesión o custodia, los sujetos obligados deberán identificar las disposiciones constitucionales o legales que expresamente así lo dispongan.

1) Información Pública Clasificada: Se trata de Información que, siendo pública, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica y que por lo tanto no debe ser publicada, salvo que el titular de los derechos haya consentido en la revelación de sus datos personales o privados (siempre que la autorización sea previa, expresa e informada) o bien cuando es claro que la información fue entregada como parte de aquella información que debe estar bajo el régimen de publicidad aplicable. Por lo tanto, se puede exceptuar el acceso al ciudadano siempre que se trate de las circunstancias legítimas y necesarias y que los derechos particulares o privados señalados en el artículo 18 de la Ley de Transparencia o en la Ley de Protección de Datos Personales, estén expuestos a un riesgo potencial en caso de que tal información fuese revelada.

2) Información Pública Reservada: Es aquella cuyo acceso podrá ser rechazado o denegado, de manera motivada y por escrito, siempre que dicho acceso estuviere expresamente prohibido por una norma legal o constitucional, el Sujeto Obligado puede restringir el acceso a esta Información Pública, debido a que puede causar daño a los intereses públicos previstos en la Ley de Transparencia. Por lo tanto, se debe verificar que la publicación de la información genere un daño potencial (que tenga la posibilidad real, probable y específica de dañar esos intereses) y significativo a alguno de los siguientes intereses públicos; que el acceso esté prohibido por una

norma constitucional o legal; y que se observen las disposiciones de la Ley de Transparencia.

Intereses que justifican la Reserva de la Información Pública

a) Defensa y seguridad Nacional; Seguridad Pública y relaciones internacionales
b) Prevención, investigación y persecución de los delitos y las faltas disciplinarias
c) El debido proceso y la igualdad de las partes en los procesos judiciales; la administración efectiva de la justicia
d) Los derechos de la infancia y la adolescencia.
e) La estabilidad macroeconómica y financiera del país.
f) La salud pública.

3) Información de Inteligencia y Contrainteligencia.

Los organismos de inteligencia y Contrainteligencia Militar (CGDJ2 en el COGFM), para la protección de la información de su competencia (Ley 1621 de 2013), establecerán los siguientes controles:

a) Toda la información deberá ser identificada, clasificada y documentada con base en los criterios de clasificación definidos en el Decreto 1070 de 2015 y Disposición No. 002 de 2014 que aprobó el Manual de Contrainteligencia Estratégica Militar y todas las normas que las modifiquen adicionen.
b) Clasificación de seguridad: Es el nivel de seguridad asignado a una información contenida, manejada o registrada por cualquier medio, según su incidencia o importancia respecto de la seguridad nacional, institucional, operacional o personal, realizada por los organismos de Inteligencia y Contrainteligencia autorizados.
c) Los niveles de clasificación de seguridad y acceso a la información serán los siguientes:

(1) Ultrasecreto: Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar al exterior del país los intereses del Estado o las relaciones internacionales, los documentos e informaciones del nivel Ultrasecreto pueden ser:

(a) El aseguramiento de la consecución de los fines esenciales del Estado, la vigencia del régimen democrático, la integridad territorial, la soberanía, la seguridad y la defensa de la Nación.
(b) La protección de las instituciones democráticas de la República, así como los derechos de las personas residentes en Colombia y de los ciudadanos colombianos en todo tiempo y lugar -en particular los derechos a la vida y la integridad personal- frente a amenazas tales como el terrorismo, el crimen organizado, el narcotráfico, el secuestro, el tráfico de armas, municiones, explosivos y otros materiales relacionados, el lavado de activos, y otras amenazas similares.
(c) La protección de los recursos naturales y los intereses económicos de la Nación. Los documentos e informaciones del nivel Ultrasecreto, pueden ser:
- Apreciaciones inteligencia de orden internacional.
- Informes de Inteligencia y contrainteligencia estratégicos.

- Informes sobre relaciones de inteligencia con otros países.
- Informes de inteligencia vital para la estabilidad del país.
- Planes de Inteligencia Nacional.
- Planes estratégicos de Inteligencia y contrainteligencia
- Planes de operaciones de Inteligencia a nivel Fuerza o superior.
- Planes de operaciones de inteligencia de cobertura a nivel frontera.

(2) Secreto: Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar al interior del país los intereses del Estado, los documentos e informaciones del nivel Secreto, pueden ser:

(a) Apreciaciones de inteligencia de orden nacional
(b) Archivo operacional de inteligencia y contrainteligencia.
(c) Códigos, equipos y material criptográfico.
(d) Estudios de contrainteligencia de instalaciones militares.
(e) Informes de operaciones de inteligencia y contrainteligencia.
(f) Orden de batalla del enemigo.
(g) Planes de contrainteligencia de cubierta, decepción y engaño.
(h) Planes de inteligencia de interés estratégico y táctico de orden interno.
(i) Planes de operaciones de inteligencia de orden interno.
(j) Planes de inteligencia y contrainteligencia.
(k) Información sobre procedimientos de Inteligencia y Contrainteligencia.

(3) Confidencial: Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar directamente las instituciones democráticas, los documentos e informaciones del nivel Confidencial, pueden ser:

(a) Informes de inteligencia sobre posibles ataques terroristas a otras instituciones del Estado.
(b) Informes de contrainteligencia sobre infiltración y/o penetración a organismos de control y autoridades civiles y judiciales por parte de organizaciones al margen de la ley.
(c) Informes de apreciaciones de la amenaza, análisis de riesgos, evaluaciones de credibilidad y confiabilidad, que se efectúen en apoyo a funcionarios y dependencias de entidades estatales.

(4) Restringido: Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información de las instituciones militares, de la Policía Nacional o de los organismos y dependencias de inteligencia y contrainteligencia, sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar en las citadas instituciones y organismos, su seguridad, operaciones, medios, métodos, procedimientos, integrantes y fuentes, los documentos e informaciones del nivel Restringido, pueden ser:

(a) Directivas y circulares de interés general para los organismos de inteligencia y contrainteligencia.
(b) Escalafones de personal militar y civil al servicio de los organismos de inteligencia y contrainteligencia de las Fuerzas Militares
(c) Estudios de credibilidad y confiabilidad del personal orgánico de los organismos de inteligencia y contrainteligencia de las Fuerzas Militares
(d) Hojas de vida del personal que labora en los organismos de inteligencia y contrainteligencia de las Fuerzas Militares.
(e) Información de carácter personal que labora en los organismos de inteligencia y contrainteligencia de las Fuerzas Militares.
(f) Nóminas de personal militar y civil al servicio de los organismos de inteligencia y contrainteligencia de las Fuerzas Militares.
(g) Normas e instrucciones para el personal al servicio de los organismos de inteligencia y contrainteligencia de las Fuerzas Militares
(h) Manuales para conocimiento exclusivo del personal de los organismos de inteligencia y contrainteligencia de las Fuerzas Militares.

d) Los jefes de los organismos de inteligencia y contrainteligencia de las Fuerzas Militares son responsables de aplicar y hacer cumplir el nivel de clasificación de cada activo de información.
e) No pueden tramitarse por sistemas electrónicos de gestión documental, los documentos elaborados por los organismos de inteligencia y contrainteligencia de las Fuerzas Militares.
f) Autorización niveles de acceso a información clasificada: Para autorizar el acceso a información clasificada los organismos de inteligencia y contrainteligencia de las Fuerzas Militares deben tener en cuenta los siguientes criterios:

(1) Expedir la tarjeta de autorización de acceso a información clasificada a los funcionarios de los organismos de inteligencia y contrainteligencia previo cumplimiento de los siguientes requisitos: estudio de credibilidad y confiabilidad, acta de posesión y funciones del cargo u obligaciones contractuales, acta de compromiso de reserva.
(2) La autorización para el acceso a los diferentes niveles de clasificación (ULTRASECRETO, SECRETO, CONFIDENCIAL y RESTRINGIDO), será otorgada por el jefe del organismo de inteligencia y contrainteligencia militar.
(3) Las tarjetas de autorización de acceso a los niveles ULTRASECRETO y SECRETO se actualizarán cada seis (6) meses; las de los niveles CONFIDENCIAL y RESTRINGIDO cada año, previo cumplimiento de los filtros de seguridad.
(4) A mayor nivel de clasificación de seguridad de la información de inteligencia y contrainteligencia, mayores serán las restricciones y controles para el acceso a la misma por parte de los servidores públicos o contratistas que deban conocer de ella.
(5) La autorización del acceso a información clasificada de inteligencia y contrainteligencia en el nivel asignado, no implica que se tenga derecho a conocer toda la información de dicha clasificación, se debe mantener el principio de la compartimentación.
(6) Para obtener la autorización de acceso a información clasificada, los funcionarios o contratistas deben acreditar el conocimiento de las políticas de seguridad de la información de los organismos de inteligencia y contrainteligencia de las Fuerzas Militares.

g) Elaboración, trámite, difusión y archivo de documentos clasificados de Inteligencia y Contrainteligencia.

(1) Elaboración

(a) Para la elaboración de productos o documentos los organismos de inteligencia y contrainteligencia de las Fuerzas Militares deben cumplir con lo consagrado en la Ley 1621 de 2013 y decreto reglamentario 1070 de 2015.

(b) Para el caso del CGDJ2 en el COGFM se debe cumplir con el "Procedimiento para la elaboración de documentos de inteligencia" MDN-COGFM-PRODIROP-CGDJ2-PT 95 1.4.

(2) Trámite y Difusión

(a) Registro en el sistema de documentos clasificados de inteligencia y contrainteligencia.
(b) Tramite firma Jefe dependencia a través de Oficial de Seguridad o Ayudante.
(c) Trámite interno en sobre cerrado marcado y solo puede ser abierto por Jefe dependencia.
(d) Trámite externo en doble sobre; Sobre interior marcado con sello clasificación; sobre exterior con los datos del Reglamento de Archivo y Correspondencia FF.MM. y sin ninguna señal de clasificación.
(e) Trámite de firmas en carpeta con carátula seguridad, control con planilla y firma de quien recibe documento.
(f) Una vez actuado por Jefe dependencia, debe descargarse del registro interno y tramitarse en sobre original sellado o grapado.
(g) Una vez aprobado por el jefe, debe regresar a la dependencia de registro del organismo de Inteligencia y Contrainteligencia, para el trámite pertinente.
(h) El personal del organismo de inteligencia y contrainteligencia que interviene en trámite debe tener tarjeta autorización para manejar documentos clasificados, promesa de reserva y evaluación técnica de confiabilidad.
(i) Para el trámite por medio electrónico, es obligatoria su encriptación, por medio del sistema autorizado.
(j) No tramitar por sistemas electrónicos de gestión documental (Sistema de registro de cada Fuerza).
(k) En el trámite de documentos clasificados debe primar la protección de la información sobre cualquier otra circunstancia.
(l) La documentación clasificada de nivel SECRETO y ULTRASECRETO, se debe enviar en sobre de seguridad, entregado personalmente al destinatario firmando planilla de entrega de acuerdo a gestión documental y acta de traspaso de reserva de la información. Este tipo de información no debe ser enviada por empresas de correo comerciales.

(3) No Publicación

Los documentos originados procesados y producidos en los organismos de inteligencia y contrainteligencia, solo se podrá difundir a los receptores legales autorizados, según lo establecido en la Ley 1621 de 2013.

(4) Archivo y Consulta

(a) Los documentos clasificados en los niveles SECRETO y ULTRASECRETO deben archivarse bajo custodia en Bóveda de Seguridad.
(b) Los documentos clasificados en los niveles CONFIDENCIAL y RESTRINGIDO deben archivarse en las dependencias de los organismos de inteligencia y contrainteligencia de las Fuerzas Militares con las debidas medidas de seguridad.
(c) Los documentos clasificados de inteligencia y contrainteligencia deben transferirse a un archivo central exclusivo para tal fin, diferente al de los documentos de otras dependencias.
(d) Los organismos de inteligencia y contrainteligencia militar deben disponer la dependencia adecuada donde pueda funcionar el mencionado archivo.
(e) El archivo de los documentos clasificados de inteligencia y contrainteligencia debe ceñirse a las normas establecidas en la Ley 594 de 2000 por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
(f) La consulta y copia de los documentos de inteligencia y contrainteligencia debe ser autorizada únicamente por el Jefe del organismo respectivo.
(g) Para la consulta se debe acreditar autorización y tarjeta para manejar documentos clasificados de inteligencia y contrainteligencia en el nivel que corresponda.
(h) Ningún documento o borrador de los niveles SECRETO y ULTRASECRETO puede retirarse de la Bóveda de Seguridad.

(5) Eliminación: Para los organismos de inteligencia y contrainteligencia aplica el ordenamiento jurídico de la Ley 594 de 2000, Ley 1621 de 2013, Decreto 1070 de 2015, Decreto 2149 de 2017, Acuerdo 010 de 2018 y Sentencia C-540 de 2012 de la Corte Constitucional.

(a) El Oficial de Seguridad y/o Suboficial Custodio del organismo de inteligencia y contrainteligencia deben verificar la eliminación total documento.
(b) Se deben utilizar máquinas trituradoras y/o picadoras de papel
(c) No deben quedar residuos que revelen el contenido
(d) No hacer reciclaje con hojas de documentos clasificados de inteligencia y contrainteligencia.
(e) La eliminación de los documentos de inteligencia y contrainteligencia, debe incluir borradores y notas manuscritas
(f) Se debe efectuar el control de residuos de documentos de inteligencia y contrainteligencia en canecas o depósitos de basura para evitar la fuga de información.

(6) Seguridad en la difusión de productos e información de inteligencia y contrainteligencia.

(a) Para la difusión de productos e información de inteligencia y contrainteligencia se deben cumplir los criterios de seguridad y restricciones (DE SOLO

CONOCIMIENTO y DE USO EXCLUSIVO) dispuestos en el artículo 2.2.3.7.1. del Decreto 10170 de 2015 "Único Reglamentario del Sector Administrativo de Defensa"

(b) Cuando se ordene al organismo de inteligencia y contra inteligencia, dar respuesta legal a un requerimiento de información de inteligencia, se debe verificar previamente lo dispuesto en el artículo 2.2.3.7.2. del Decreto 10170 de 2015 "Único Reglamentario del Sector Administrativo de Defensa"

c. Gestión de Medios Removibles

Todos los funcionarios del Comando General, son responsables del cumplimiento de esta política mediante la cual, se genera la obligatoriedad para que se realice la devolución de los activos de la información a cada responsable de los centros de costos o líder de proceso, una vez finalizado su compromiso contractual.

1) Se restringe la conexión no autorizada a la infraestructura tecnológica del Sector Defensa, de cualquier elemento de almacenamiento como dispositivos personales USB, discos duros externos, DVD, cámaras fotográficas, cámaras de video, teléfonos celulares, módems, entre otros dispositivos no institucionales.
2) Los medios de almacenamiento removibles como cintas, discos duros, CDs, DVDs, dispositivos USB, entre otros, así como los medios impresos que contengan información institucional, deben ser controlados y físicamente protegidos.
3) Las instituciones y entidades que conforman el Sector Defensa definirán los medios removibles de almacenamiento que podrán ser utilizados por las personas autorizadas en los sistemas de información y en la plataforma tecnológica, en caso de ser requerido para el cumplimiento de sus funciones.
4) Cada medio removible de almacenamiento deberá estar identificado de acuerdo con el tipo de información que almacene, dando cumplimiento a los lineamientos establecidos en el procedimiento de Inventario y Clasificación de Activos de Información.
5) Si un medio removible llegase a contener información con distintos niveles de clasificación, será clasificado con la categoría que posea el mayor nivel de clasificación.
6) Para los procesos de baja, de reutilización o de garantía de los dispositivos que contengan medios de almacenamiento, se debe cumplir según sea el caso con la destrucción física del mismo o borrado seguro. La destrucción segura se documentará mediante acta, registro fílmico y fotográfico.
7) El tránsito o préstamo de medios removibles deberá ser autorizado por el propietario de dicho activo.

d. Dispositivos Móviles.

1) Para el uso de dispositivos institucionales de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, se debe implementar controles de acceso y técnicas criptográficas para cifrar la información crítica almacenada en estos.
2) La conexión de los dispositivos móviles a la infraestructura tecnológica institucional deberá ser debidamente autorizada por la oficina de tecnología, o la que haga sus

veces, previa verificación de que cuenten con las condiciones de seguridad, estableciendo los mecanismos de control necesarios para proteger la infraestructura.

e. Uso Adecuado de los Activos de las Información.

Cada Jefatura, Subjefaturas, Departamento, Dirección y Unidades del Comando General de las Fuerzas Militares, podrán monitorear y supervisar la información, sistemas, servicios y equipos que sean de su propiedad, de acuerdo con lo establecido en esta política y la legislación vigente.

1) Internet:

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

a) Navegación en sitio de contenido sexualmente explicito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos.
b) Publicación, envío o adquisición de material sexualmente explica, discriminatorio o de cualquier otro contenido que se considere fuera de los límites permitidos.
c) Publicación o envío de información confidencial hacia afuera de las instituciones y entidades del Sector Defensa sin la aplicación previa de los controles para salvaguardar la información y sin la autorización de los propietarios respectivos.
d) Utilización de otros servicios disponibles a través de Internet que permitan establecer conexiones o intercambios no autorizados.
e) Publicación de anuncios comerciales o material publicitario, salvo las oficinas que dentro de sus funciones así lo requieran. Lo anterior deberá contemplar una solicitud previa, la cual debe ser justificada por el jefe de la oficina.
f) Promover o mantener asuntos o negocios personales.
g) Descarga, instalación y utilización de programas de aplicación o software no relacionados con la actividad laboral y que afecte el procesamiento de la estación de trabajo o de la red.
h) Navegación en las cuentas de correo de carácter personal, no institucional, o en redes sociales, sin una justificación por parte de la Entidad.
i) Uso de herramientas de mensajería instantánea no autorizadas por la oficina de tecnología, o la que haga sus veces.
j) Emplear cuentas de correo externas no corporativas para el envío o recepción de información institucional.

Se realizará monitoreo permanente de tiempos de navegación y páginas visitadas por los funcionarios y terceros autorizados. Así mismo, se puede inspeccionar, registrar e informar las actividades realizadas durante la navegación.

El uso de Internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información.

2) Correo electrónico institucional o corporativo:

La cuenta de correo electrónico institucional debe ser usada para el desempeño de las funciones asignadas dentro de cada una de las instituciones y entidades que conforman el Comando General de las Fuerzas Militares y estará bajo la responsabilidad del Departamento Conjunto de Comunicaciones.

a) La cuenta de correo electrónico institucional debe ser usada para el desempeño de las funciones asignadas.
b) El tamaño de los buzones y mensajes de correo serán determinados por el Departamento Conjunto de Comunicaciones CGDJ6, o quien hagan sus veces, conforme a las necesidades de cada usuario y previa autorización del jefe inmediato.
c) En cada institución y entidad se suministrará una cuenta de correo corporativa por cada oficina que lo requiera, la cual será utilizada para él envió masivo de correos institucionales.
d) No se considera aceptado el uso del correo electrónico corporativo para los siguientes fines:

(1) Enviar o retransmitir cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.
(2) El envío de cualquier tipo de archivo que ponga en riesgo la seguridad de la información: en caso que sea necesario hacer un envío de este tipo de archivos deberá contar con la autorización correspondiente por parte de la oficina de tecnología, o la que haga sus veces.
(3) El envío de información relacionada con la defensa y la seguridad nacional a otras entidades del Gobierno diferentes a las que conforman el Sector Defensa, sin la autorización previa del propietario de la información y de la oficina de tecnología, o la que haga sus veces.

e) Toda información que requiera ser transmitida fuera de cada institución y entidad del sector, y que por sus características de confidencialidad e integridad debe ser protegida, debe estar en formatos no editables y con mecanismos de seguridad. *Sólo puede ser enviada en el formato original bajo la responsabilidad del usuario* y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

f) Todo correo electrónico deberá respetar el estándar de formato e imagen corporativa definido para cada una de las instituciones y entidades del Sector Defensa y deberá contener al final del mensaje un texto en español e inglés en el que se contemplen, mínimo, los siguientes elementos:

(1) El mensaje (incluyendo cualquier anexo) contiene información confidencial y se encuentra protegido por la Ley.
(2) El mensaje sólo puede ser utilizado por la persona o empresa a la cual está dirigido.
(3) En caso de que el mensaje sea recibido por alguna persona o empresa no autorizada, solicitar borrarlo de forma inmediata.
(4) Prohibir la retención, difusión, distribución, copia o toma de cualquier acción basada en el mensaje.

3) Redes Inalámbricas:

a) Se debe propender por la implementación de ambientes de trabajo completamente independientes para la red operativa y la red con servicio de internet a fin de minimizar los riesgos de intrusión a las redes institucionales.
b) Los usuarios de las redes inalámbricas deben ser sometidos a las mismas condiciones de seguridad de las redes cableadas en lo que respecta a identificación, autenticación, control de contenido de internet y cifrado entre otros.
c) El servicio de Internet en las Escuelas de Formación y Capacitación, deberá contar con mecanismos de autenticación de usuarios y deberá estar configurado de tal manera que permita el desarrollo de las actividades académicas y de investigación.
d) El servicio de internet en las escuelas de formación, capacitación y en las instalaciones destinadas para el bienestar social, deben estar configuradas de forma independiente a la red operativa de la institución o entidad del Sector Defensa.
e) Se debe implementar infraestructura inalámbrica que permita configuraciones de seguridad. En ningún caso se podrá dejar las configuraciones y contraseñas establecidas por defecto.

4) Segregación de Redes:

a) La plataforma tecnológica critica de las instituciones y entidades del Sector Defensa que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet.

b) La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos, de enrutamiento y de seguridad, si así se requiere. La Oficina de Tecnología, o la que haga sus veces, es la encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

5) Computación en la Nube (Cloud Computing)

a) Por ningún motivo se podrá almacenar información clasificada en servicios en la nube públicos o híbridos.

b) Ningún servicio de carácter operativo e institucional de las instituciones y entidades del Sector Defensa, deberán ser contratados en servicios en la nube públicos o híbridos.
c) Para el caso de las escuelas de formación y capacitación se podrá hacer uso de servicios en la nube públicos e híbridos, siempre y cuando no se vea comprometida la seguridad institucional o información clasificada.
d) Para el caso de las escuelas de formación y capacitación se podrá hacer uso de servicios en la nube públicos e híbridos, siempre y cuando no se vea comprometida la seguridad institucional o información clasificada.
e)

6) Sistemas de Información de Acceso Público y Normas de Transparencias del Comando General de las Fuerzas Militares.

a) La información pública producida, deberá estar resguardada de posibles modificaciones que afecten la imagen institucional.
b) Todo portal institucional, deberá contener la política de privacidad y uso, así como la política de seguridad del mismo.
c) Deberán garantizar el derecho de Habeas Data al público que hace uso de los servicios de sus respectivos portales institucionales y propender por la seguridad de la información ingresada a través de ellos, aclarando que no se es responsable de la veracidad de la misma.
d) Toda la información publicada en los portales institucionales, o en cualquier otro medio, deberá contar con la revisión y aprobación de la Oficina de Comunicaciones Estratégicas, o similares, y deberá estar debidamente rotulada según su nivel de clasificación.

7) Recursos tecnológicos:

a) La instalación de cualquier tipo de software en los equipos de cómputo de cada institución y entidad que conforma el Sector Defensa es responsabilidad exclusiva de sus Oficinas de Tecnología, o las que hagan sus veces, por tanto son los únicos autorizados para realizar esta labor.
b) Ningún activo de información debe ser instalado con la configuración establecida por defecto por el fabricante o proveedor, incluyendo cuentas y claves de administrador.
c) Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla no definido. Estos cambios pueden ser realizados únicamente por las Oficinas de Tecnología, o las que hagan sus veces, de las correspondientes instituciones y entidades que conforman el Sector Defensa.
d) Los usuarios no deben realizar cambios físicos en las estaciones de trabajo, tales como, cambio de ubicación, mantenimientos, repotenciación, modificaciones en su configuración física. Estas actividades sólo podrán ser realizadas por las Oficinas de Tecnología, o las que hagan sus veces.
e) Los equipos de cómputo asignados, deben ser devueltos a la dependencia responsable una vez sean reemplazados o cuando el funcionario o tercero

responsable de dicho equipo finalice su vinculación con la entidad del sector para la que estuviere prestando sus servicios.

f) De acuerdo con el literal anterior, las dependencias no deben almacenar equipos de cómputo en las oficinas una vez haya cesado el uso de los mismos.

3. Gestión Control de Acceso.

Esta política hace referencia a aquellas directrices mediante las cuales el Comando General de las Fuerzas Militares ha implementado los procedimientos frente a la administración y responsabilidades, relacionados con los accesos a la información sin importar si estos sean electrónicos o físicos así:

a. Control de Acceso con usuarios y Contraseñas:

1) Los sistemas de información y dispositivos de procesamiento, seguridad informática y comunicaciones contarán con mecanismos de identificación de usuarios y procedimientos para el control de acceso a los mismos.
2) El acceso a los activos de información institucionales estará permitido únicamente a los usuarios autorizados por el propietario de cada activo, según el procedimiento *Gestión de Usuarios y Contraseñas*.
3) Cualquier usuario interno o externo que requiera acceso remoto a la red o a la infraestructura de procesamiento o seguridad informática del Sector Defensa deberá estar autorizado por la respectiva Oficina de Tecnología, o la que haga sus veces.
4) Todas las conexiones remotas deberán ser autenticadas y seguras antes de conceder el acceso, el tráfico de datos deberá estar cifrado.
5) La creación, modificación y baja de usuarios en la infraestructura de procesamiento de información, comunicaciones y seguridad informática deberá seguir el procedimiento Gestión de Usuarios y Contraseñas.
6) Todo usuario que se cree para que un tercero ingrese a las redes de las instituciones y entidades del Sector Defensa, debe tener una fecha de vencimiento específica, la cual en ningún caso debe superar la fecha de terminación de sus obligaciones contractuales.
7) La asignación de privilegios en las aplicaciones para los diferentes usuarios estarán determinados por el procedimiento Gestión de Usuarios y Contraseñas. Estos privilegios deben revisarse a intervalos regulares y ser modificados o reasignados cuando se presenten cambios en el perfil del usuario, ya sea por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral.
8) Los equipos de terceros que requieran acceder a la redes de datos de las diferentes instituciones y entidades que conforman el Sector Defensa deben cumplir un procedimiento de sanitización informática antes de concedérseles dicho acceso.
9) Los equipos de terceros que hayan sido autorizados para acceder de forma permanente a una o varias de las redes de datos institucionales, sólo podrán hacerlo una vez se haya cumplido con el formateo inicial de discos duros y/o medios de almacenamiento; posteriormente, deben permanecer dentro de las respectivas instalaciones hasta la finalización del contrato o las labores para las cuales estaba

definido. Una vez culminadas estas labores se debe proceder a un formateo final para retirar estos equipos de las instalaciones.

10) Los accesos a la red inalámbrica deberán ser autorizados por la respectiva Oficina de Tecnología, o la que haga sus veces, previa verificación de que cuenten con las condiciones de seguridad, estableciendo mecanismos de control necesarios para proteger la infraestructura.

b. Gestión de Contraseñas

1) La administración así como la asignación y entrega de las contraseñas a los usuarios deberá seguir el procedimiento Gestión de Usuarios y contraseñas.
2) Los usuarios deberán seguir las siguientes reglas para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:

   a) Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.
   b) Las contraseñas no deberán ser reveladas.
   c) Las contraseñas no se deberán escribir en ningún medio, excepto para los casos de administradores, cuando son entregadas en custodia de acuerdo con el procedimiento Gestión de Usuarios y Contraseñas.
   d) Es deber de cualquier funcionario y tercero reportar cualquier sospecha de que una persona esté utilizando un usuario y contraseña que no le pertenece, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.

c. Bloqueo de Sesión, Escritorio y Pantalla

1) En horas no hábiles, o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar los medios que contengan información crítica protegida bajo llave.
2) Los usuarios deberán bloquear su estación cada vez que se retiren de su puesto de trabajo y sólo se podrá desbloquear con la contraseña del mismo usuario que la bloqueó.
3) Todas las estaciones de trabajo deberán usar únicamente el papel tapiz y el protector de pantalla establecido por la respectiva institución y entidad del sector.
4) Los usuarios no deberán almacenar en el escritorio de sus estaciones de trabajo documentos, accesos directos a los mismos o a sistemas de información sensibles.
5) Los usuarios son responsables por la custodia y las acciones que se realicen a través de los activos informáticos asignados, por lo tanto debe estar presente en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización de dichos activos.

d. Control de Versiones

1) Antes de la puesta en producción de una aplicación nueva, o de la modificación de las plataformas existentes, se debe asignar un número de edición o versión a la misma, de acuerdo con el procedimiento Control de Versiones (Anexo Q).
2) El método de enumeración de las versiones deberá distinguir entre versiones en producción, en etapa de desarrollo, en etapa de pruebas o versión archivada.
3) Todas las versiones deben ser almacenadas en bibliotecas, repositorios o directorios y deben contar con controles de acceso lógicos donde sólo se permita el acceso al personal autorizado.
4) Periódicamente, las versiones que se encuentran en los ambientes de producción deben ser verificadas contra los repositorios y la documentación de los controles de cambio con el fin de determinar si los dos son congruentes. Si llegase a presentarse incongruencia en la revisión realizada, esto será identificado como un incidente de seguridad y se atenderá de acuerdo con el procedimiento de Gestión de Incidentes de seguridad.

e. Perímetro de Seguridad

El Departamento de Seguridad del Comando General de las Fuerzas Militares, junto con Departamento de Inteligencia y Contra Inteligencia y los líderes de procesos definirá la política de los perímetros físicos de seguridad donde se encuentre la información crítica, sensible o se realice almacenamiento, el cual se establecerá los protocolos de ingresos a estas áreas restringidas.

De igual forma definirá las áreas de carga donde se especifique los protocolos para la recepción física de los paquetes, correspondencia, bodegaje y otros servicios que requiere la entidad, para evitar el acceso no autorizado de terceros a estas áreas protegidas.

4. Controles Criptográficos

El Departamento Conjunto de Comunicaciones, o las que hagan sus veces, de las instituciones y entidades que conforman el Comando General de las Fuerzas Militares, deben identificar, definir e implementar mecanismos y controles criptográficos para garantizar el cumplimiento de los objetivos de seguridad definidos, en términos de protección de la confidencialidad de la información en medio electrónico, de acuerdo con los lineamientos definidos en el procedimiento de Inventario y Clasificación de Activos de Información, tanto cuando se encuentra almacenada como cuando es transmitida o procesada, teniendo en cuenta la clasificación y sensibilidad de la información.

No se permite el uso de herramientas o mecanismos de cifrado de información diferentes a las autorizadas por las Oficinas de Tecnología, o las que hagan sus veces, los cuales deben estar documentados en una lista de software autorizado que sea divulgada a todos los funcionarios y terceros autorizados.

5. Seguridad Física y del Entorno

a. Acceso Físico

1) Se evaluarán las necesidades de capacitación e implementación de los procedimientos y controles necesarios para garantizar la integridad, disponibilidad y confidencialidad de los activos de información.
2) Todas las puertas que utilicen sistema de control de acceso, deberán permanecer cerradas, y es responsabilidad de todos los funcionarios y terneros autorizados evitar que las puertas se dejen abiertas.
3) Se debe exigir a todo el personal, sin excepción, el porte en un lugar visible del mecanismo de identificación adoptado para ellos por cada una de las instituciones y entidades que conforman el sector, mientras permanezcan dentro de sus instalaciones.
4) Los visitantes deberán permanecer acompañados de un funcionario cuando se encuentren dentro de alguna de las áreas seguras.
5) Es responsabilidad de todos los funcionarios y terceros acatar las normas de seguridad y mecanismos de control de acceso a las instituciones y entidades del Sector Defensa.
6) Los funcionarios y terceros, así como los visitantes, deberán tener acceso físico restringido a los sitios que requieran y les sean autorizados para el cumplimiento de sus funciones, tareas o misión dentro de las instalaciones.

b. Protección de los Activos.

1) Copias de Respaldo

a) Se debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por las Oficinas de Tecnología, o las que hagan sus veces, y las dependencias responsables de la misma, contenida en la plataforma tecnológica de las instituciones y entidades del Sector Defensa, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad, según lo definido en el procedimiento Gestión de Copias de Respaldo y recuperación.
b) Los medios de las copias de respaldo se almacenarán 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.
c) Se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares, establecidos según las necesidades y capacidades de cada una de las instituciones y entidades del Sector por sus correspondientes oficinas de tecnología, o las que hagan sus veces, con el fin de asegurar que son confiables en caso de emergencia. Estas copias serán retenidas

por un periodo de tiempo determinado, de acuerdo a lo establecido en el procedimiento de Gestión de Copias de Respaldo.

d) Las Oficinas de Tecnología, o las que hagan sus veces, establecerán procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca de su traslado, frecuencia e identificación; así mismo, definirá conjuntamente con las dependencias usuarias los periodos de retención de dicha in formación.
e) Se debe 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 para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada

c. Retiro de Activos

1) El retiro de equipos o medios que procesan o almacenan algún tipo de información y/o que hacen parte de la plataforma tecnológica, debe ser autorizado por el propietario del activo previa solicitud del funcionario interesado. Si el activo está clasificado como relacionado con la defensa y la seguridad nacional, el retiro deberá estar autorizado también por el Ayudante General (o quién haga sus veces).
2) Todo equipo, medio de almacenamiento, información o software que requiera ser retirado de las instalaciones de las instituciones y entidades del Sector Defensa, debe ser debidamente identificado y registrado antes de conceder la autorización respectiva.
3) Las instituciones y entidades que conforman el Sector Defensa proporcionarán los mecanismos y recursos necesarios para que en cada punto de acceso a sus instalaciones exista un puesto de revisión donde se inspeccione y se lleve el control de los equipos que son ingresados y retirados.
4) Los equipos de terceros que hayan sido autorizados para acceder a las redes de datos sólo podrán ser retirados al finalizar el contrato o las labores para las cuales estaba definido, previo borrado seguro de la información a través del proceso de sanitización. Las Oficinas de Tecnología, o las que hagan sus veces, de las instituciones y entidades que conforman el Sector Defensa, generarán un paz y salvo como constancia de dicho proceso, que deberá ser presentado al momento del retiro del equipo de las instalaciones físicas correspondientes.

d. Seguridad y Mantenimiento de los Equipos

1) Los equipos que hacen parte de la infraestructura tecnológica de las instituciones y entidades que conforman el Sector Defensa deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos.
2) Las instituciones y entidades que conforman el Sector Defensa adoptarán los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo entre otros.

3) Los funcionarios y terceros velarán por el uso adecuado de los equipos de escritorio, portátiles y móviles que les hayan sido asignados, por lo tanto, dichos equipos no deberán ser prestados a personas ajenas o no autorizadas.
4) Se debe asegurar que, sobre la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática, se realicen mantenimientos periódicos con el fin de que dichas actividades no se vean afectadas por obsolescencia. Por lo tanto, revisará constantemente la vida útil de cada uno de los recursos que componen dicha infraestructura de acuerdo con la descripción y recomendaciones de sus fabricantes.
5) Los equipos tales como máquinas de copiado, impresoras y máquinas de fax deberán estar ubicados en zonas de acceso restringido y se permitirá el uso únicamente a personal autorizado.
6) Los equipos portátiles deberán estar asegurados (cuando estén desatendidos) con la guaya o el mecanismo que se defina para su protección, sea dentro o fuera de las instalaciones de las instituciones y entidades que conforman el Sector Defensa.
7) Las instituciones y entidades que conforman el Sector Defensa garantizarán la existencia de pólizas o seguros para la reposición de los activos informáticos que respaldan los planes de contingencia y la continuidad de los servicios.

e. *Seguridad de los Equipos Fuera de las Instalaciones*

1) Los usuarios que requieran manipular los equipos o medios fuera de las instalaciones de cada una de las instituciones y entidades que conforman el Sector Defensa, deben velar por la protección de los mismos sin dejados desatendidos, comprometiendo la imagen o información del sector.
2) El propietario del activo, con el apoyo de la oficina de tecnología o la que haga sus veces, identificará mediante una metodología de análisis de riesgos que cada institución o entidad establezca, los riesgos potenciales que puede generar el retiro de equipos o medios de las instalaciones: así mismo, adoptará los controles necesarios para la mitigación de dichos riesgos.
3) En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información relacionada con la defensa y la seguridad nacional, se deberá realizar inmediatamente el respectivo reporte de acuerdo con el procedimiento gestión de incidentes de seguridad y se deberá poner la denuncia ante la autoridad competente, si aplica.
4) Los equipos de cómputo o activos de información que por razones del servicio se retiren de las instalaciones de las instituciones y entidades que conforman el Sector Defensa, deberán contener únicamente la información estrictamente necesaria para el cumplimiento de su misión y se deshabilitarán los recursos que no se requieren o que puedan poner en riesgo la información que contiene.

f. Documentación de Procedimientos Operativos

1) La ejecución de cualquier actividad asociada con la infraestructura tecnológica para el procesamiento de información, comunicaciones y seguridad informática debe estar

soportada por instrucciones o procedimientos operativos documentados, los cuales siempre deben estar a disposición de todos los usuarios que los necesiten para el desarrollo de sus labores.

2) Los procedimientos operativos deben quedar documentados con instrucciones detalladas, teniendo en cuenta el procesamiento y manejo de información, instrucciones para el manejo de errores, contactos de soporte en caso de dificultades técnicas u operativas inesperadas, así como instrucciones para el manejo de medios y exposición de resultados especiales y de carácter confidencial.
3) La elaboración, publicación y modificación que se realice de los documentos debe ser autorizada por el administrador de la aplicación, propietario del activo, Jefe de dependencia o el funcionario a quien se le hayan otorgado dichas funciones.
4) Los procedimientos operativos deben contener instrucciones para el manejo de los errores que se puedan presentar en la ejecución de las actividades, contactos de soporte, procedimientos de reinicio y recuperación de sistemas y aplicaciones, forma de procesamiento y manejo de la información, copia de respaldo de la información y los demás a los que hubiere lugar.

6. Seguridad en las Operaciones.

a. Servicio de Cambios.

1) Todo cambio que se realice sobre los sistemas de información e infraestructura tecnológica debe ser controlado, gestionado y autorizado adecuadamente por parte de las Oficinas de Tecnología, o las que hagan sus veces, de las instituciones y entidades que conforman el Sector Defensa, y debe cumplir con una planificación y ejecución de pruebas que identifiquen riesgos e impactos potenciales asociados que puedan afectar su operación.
2) Todos los cambios que se realicen sobre los sistemas de información y la infraestructura tecnológica deberán estar precedidas de la definición de los requerimientos, especificaciones y controles definidos en el procedimiento de Control de Cambios. Dicha definición deberá ser realizada teniendo en cuenta como mínimo la confidencialidad, integridad y disponibilidad de la información.

b. Asistencia de Capacidad.

El Departamento Conjunto de Comunicaciones, o las que hagan sus veces, como áreas responsable de la administración de la plataforma tecnológica, deberán implementar los mecanismos, controles y herramientas necesarias para asegurar que los recursos que componen dicha plataforma sean periódicamente monitoreados, afinados y proyectados para futuros requerimientos de capacidad de procesamiento y comunicación, conforme a lo establecido en el Procedimiento Gestión de la Capacidad. El responsable de cada componente de la plataforma tecnológica deberá realizar el monitoreo permanente sobre este.

c. Separación de Ambientes

1) Cada una de las instituciones y entidades que conforman el Sector Defensa proveerán los mecanismos, controles y recursos necesarios para contar con niveles adecuados de separación lógica y/o física entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica y sistemas de información, con el fin de reducir el acceso no autorizado y evitar cambios que pudieran afectar su operación.
2) El paso de software y hardware, de un ambiente a otro, deberá ser controlado y gestionado de acuerdo con lo definido en el Procedimiento de Control de Cambios.
3) Los usuarios deberán utilizar diferentes perfiles para el ambiente de desarrollo, de pruebas y de producción; así mismo, se deberá asegurar que cada usuario cuente únicamente con los privilegios necesarios en cada ambiente para el desarrollo de sus funciones.
4) No deberán realizarse pruebas, instalaciones o desarrollos de hardware o software directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad o confidencialidad de la información.
5) El ambiente del sistema de prueba debe emular el ambiente de producción lo más estrechamente posible.
6) No se permite la copia de información Ultra Secreta, Secreta, Reservada, Confidencial, Restringida o Exclusiva de Comando, desde el ambiente de producción al ambiente de pruebas; en caso de que sea estrictamente necesario, la copia debe contar con las respectivas autorizaciones y se deben implementar controles que garanticen que la confidencialidad de la información sea protegida y que se elimine de forma segura después de su uso.
7) Se restringe el acceso a los compiladores, editores, utilidades de los sistemas y otras herramientas de desarrollo desde los sistemas del ambiente de producción y a cualquier usuario que no lo requiera para el desarrollo de su labor.
8) Periódicamente se deberá verificar las versiones instaladas tanto en ambiente de pruebas como en producción y se confrontará esta información con revisiones previas y con las versiones de programas fuentes almacenadas en los repositorios de cada institución y entidad del sector.

d. Protección contra Software Malicioso

1) Los sistemas operacionales y aplicaciones deberán actualizarse según lo definido en los procedimientos de Gestión de Vulnerabilidades Técnicas y Control de Cambios.
2) Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y seguridad de la información deberán estar protegidos mediante herramientas y software de seguridad que prevengan el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar posibles fallos.
3) Las herramientas y demás mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin autorización de las correspondientes Oficinas de

Tecnología, o las que hagan sus veces, y deberán ser actualizados permanentemente.

4) No está permitido escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier equipo o red institucional.
5) Todos los medios de almacenamiento que se conecten a equipos de la infraestructura de las diferentes instituciones y entidades que conforman el Sector Defensa deberán ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la seguridad de la información corporativa.
6) El código móvil sólo podrá ser utilizado si proviene de sitios de confianza y es autorizado por el área competente.
7) Cada institución y entidad que conforma el 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.
8) Los sistemas, equipos e información institucionales deberán ser revisados periódicamente para verificar que no haya presencia de código malicioso.

e. *Gestión de Vulnerabilidades Técnicas*

Las Oficinas de Tecnología, Cibernéticas o las que hagan sus veces, realizarán las revisiones de las alertas de seguridad definiendo, en caso de ser necesario, un plan de acción para mitigar el impacto de las mismas en los ambientes de producción y desarrollo de la infraestructura tecnológica.

1) Se encargarán de identificar las vulnerabilidades técnicas de las diferentes plataformas tecnológicas y para esto definirá las herramientas y/o servicios necesarios.
2) Serán responsables de proponer y ejecutar un programa de evaluación y gestión de vulnerabilidades que debe ser utilizado para la plataforma tecnológica de la institución o entidad.
3) No se permite a los usuarios de los activos informáticos, sin la autorización expresa de la oficina de tecnología, o la que haga sus veces, realizar o participar por iniciativa propia o de terceros, en pruebas de acceso o ataques activos o pasivos a los activos informáticos del Sector Defensa, o a la utilización de los mismos para efectuar pruebas de vulnerabilidad o ataques a otros equipos o sistemas externos.
4) Los administradores de las plataformas y sistemas de información serán responsables de mantener protegida la infraestructura a su cargo de los riesgos derivados de las vulnerabilidades técnicas identificadas.
5) Se realizará, por parte del área competente, el seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas.

7. Seguridad en las Comunicaciones.

   a. Aseguramiento de Servicios en la RED.

      1) Tanto los sistemas de información que manejan información crítica, como los dispositivos de procesamiento, de red y de seguridad informática deberán generar registros de eventos que serán verificados periódicamente con el fin de detectar actividades no autorizadas sobre la información, siguiendo el procedimiento Monitoreo y Revisión de "Logs".
      2) El tiempo de retención de los LOGS" estará dado por las condiciones específicas de cada sistema de información, recurso informático o dispositivo de red y por las leyes, normativas o regulaciones que rigen al Sector Defensa.
      3) El lugar de retención de los registros estará definido por el nivel de clasificación de información que posean dichos registros.
      4) Todo aquel evento que se identifique por medio del monitoreo y revisión de los registros y que ponga en riesgo la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica deberá ser reportado a la oficina de tecnología, o la que haga sus veces, mediante el procedimiento de Gestión de Incidentes de Seguridad.

   b. Transferencias de Información.

      1) Todo funcionario y/o tercero es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.
      2) Los propietarios, de información que se requiera intercambiar, son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma; por su parte, los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad de acuerdo a la reglamentación vigente.
      3) El intercambio de información y de software con otras entidades, se realiza previa celebración de convenio interadministrativo en el que se establecen cláusulas de responsabilidad, deberes y derechos.
      4) Los acuerdos de intercambio deben, en todo caso, velar por el cumplimiento de las regulaciones legales, propiedad intelectual y protección de datos personales. Asi mismo, deben especificar las consideraciones de seguridad y reserva de la información y las responsabilidades por el mal uso o divulgación de la misma.
      5) Cuando la información sea solicitada por autoridad judicial o administrativa competente; la entrega se realizará siguiendo el procedimiento establecido por la entidad que solicita la información.
      6) El intercambio de información deberá contemplar las siguientes directrices:

         a) Uso de web servicies, para la publicación y consumo de información electrónica.
         b) Uso de canales cifrados
         c) Respeto por los derechos de autor del software intercambiado.

d) Términos y condiciones de la licencia bajo la cual se suministra el software.
e) Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido por el receptor de la información.
f) Informar al titular de los datos, el intercambio de estos con otras entidades.
g) Informar sobre la propiedad de la información suministrada y las condiciones de su uso.

c. Recursos tecnológicos:

1) La instalación de cualquier tipo de software en los equipos de cómputo de cada institución y entidad que conforma el Sector Defensa es responsabilidad exclusiva de sus Oficinas de Tecnología, o las que hagan sus veces, por tanto son los únicos autorizados para realizar esta labor.
2) Ningún activo de información debe ser instalado con la configuración establecida por defecto por el fabricante o proveedor, incluyendo cuentas y claves de administrador.
3) Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla no definido. Estos cambios pueden ser realizados únicamente por las Oficinas de Tecnología, o las que hagan sus veces, de las correspondientes instituciones y entidades que conforman el Sector Defensa.
4) Los usuarios no deben realizar cambios físicos en las estaciones de trabajo, tales como, cambio de ubicación, mantenimientos, repotenciación, modificaciones en su configuración física. Estas actividades sólo podrán ser realizadas por las Oficinas de Tecnología, o las que hagan sus veces.
5) Los equipos de cómputo asignados, deben ser devueltos a la dependencia responsable una vez sean reemplazados o cuando el funcionario o tercero responsable de dicho equipo finalice su vinculación con la entidad del sector para la que estuviere prestando sus servicios.
6) De acuerdo con el literal anterior, las dependencias no deben almacenar equipos de cómputo en las oficinas una vez haya cesado el uso de los mismos.

8. Relación con los Proveedores.

a. Cuando exista la necesidad de otorgar acceso de terceras partes a las instituciones y entidades del Sector Defensa deberá realizarse, siempre con la participación del propietario de la información, una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta entre otros los siguientes aspectos:

1) El tipo de acceso requerido (físico, lógico y a qué recursos).
2) Los motivos para los cuales solicita el acceso.
3) El valor de la información.
4) Los controles empleados por la tercera parte.
5) La incidencia de este acceso en la seguridad de la información de las instituciones y entidades

b. En todos los contratos cuyo objeto sea la prestación de servicios a título personal, bajo cualquier modalidad jurídica, que deban desarrollarse dentro de las instalaciones de las instituciones y entidades, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario los permisos a otorgar.
c. En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que definan las condiciones para la conexión o el acceso.
d. El acceso de los terceros a la información o a cualquier elemento de la infraestructura tecnológica debe ser solicitado por el supervisor, o persona a cargo del tercero, al propietario de dicho activo. Este, junto con la oficina de tecnología o la que haga sus veces, aprobarán y autorizarán el acceso y uso de la información.
e. Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de computadores, contemplarán como mínimo los siguientes aspectos:

   1) Forma en los que se cumplirán los requisitos legales aplicables.
   2) Medios para garantizar que todas las partes involucradas en la tercerización incluyendo los subcontratistas, conocen sus responsabilidades en materia de seguridad.
   3) Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos.
   4) Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información Sensible.
   5) Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
   6) Niveles de seguridad física que se asignará al equipamiento tercerizado.
   7) Derecho a la auditoria por parte de las instituciones y entidades del Sector Defensa.

9. Adquisición, Desarrollo y Mantenimiento de la Información.

Este procedimiento estará bajo la responsabilidad del Departamento Conjunto de Comunicaciones CGDJ6 el cual establecerá el protocolo de la seguridad en los sistemas o adquiridos a un tercero, verificando que cada uno de ellos preserve la confidencialidad, integridad y disponibilidad de la información del Comando General de las Fuerzas Militares, dicha información de activos deberá ser especificada y actualizada por el encargado del proceso.

Se debe tener en cuenta el uso de ambientes de desarrollo, prueba y producción para los sistemas de información.

El Control de Software se realizara con personal especializado llevando el respectivo registro de control de los activos de la información, de igual forma indicara el uso, limitación y los protocolos de uso indebido no autorizado por el Comando General.

10. Gestión de Incidente de Seguridad de las Información.

a. Los funcionarios y terceros deberán informar cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.
b. Para los casos en que los incidentes reportados requieran judicialización se deberá coordinar con los organismos que cuentan con función de policía judicial.
c. Se debe establecer y mantener actualizado un directorio de los funcionarios involucrados dentro del procedimiento de Gestión de Incidentes de Seguridad para cada una de las instituciones y entidades que conforman el Sector Defensa.
d. Se debe llevar un registro detallado de los incidentes de seguridad de la información y la respuesta que fue implementada en cada uno de ellos, contemplando los daños que se causaron por el mismo y, de ser posible, la valoración de los daños.
e. Se debe propender por la adquisición de herramientas que faciliten el proceso de gestión de incidentes de seguridad de la información.
f. Los resultados de las investigaciones que involucren a los funcionarios del Sector Defensa deberán ser informados a las áreas de competencia.
g. Las instituciones y entidades que conforman el Sector Defensa deberán establecer los mecanismos de control necesarios para recolectar y preservar la evidencia de las investigaciones que se realicen durante el análisis de un incidente de seguridad de la información.

11. Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio.

a. La seguridad de la información es una prioridad y se incluye como parte de la gestión general de la continuidad del negocio y del compromiso de la Alta Dirección.
b. Las entidades que conforman el Sector Defensa deberán contar con un Plan de Continuidad del Negocio que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales.
c. Para el Sector Defensa su activo más importante es el recurso humano y por lo tanto será su prioridad y objetivo principal establecer las estrategias para mantenerlo.
d. Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades relacionados con el plan, estarán incorporados y definidos en el Plan de Continuidad de Negocio.
e. Los responsables de los procesos serán los encargados de mantenerlos documentados y actualizados e informar cualquier cambio al responsable de la gestión del Plan de Continuidad de Negocio.
f. Se describen algunas acciones identificadas que afectan la seguridad de la información y que, al poner en riesgo la disponibilidad, confidencialidad e integridad y se deben evitar:

1) Dejar los computadores encendidos en horas no laborables.
2) Permitir que personas ajenas a las instituciones y entidades del Sector Defensa, ingresen sin previa autorización a las áreas restringidas o donde se procese información sensible.
3) No clasificar y/o etiquetar la información.

4) No guardar bajo llave documentos impresos que contengan información clasificada, al terminar la jornada laboral.
5) No retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.
6) Reutilizar papel que contenga información sensible, no borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo y no garantizar que no queden documentos o notas escritas sobre las mesas.
7) Hacer uso de la red de datos de las instituciones y entidades del Sector Defensa, para obtener, mantener o difundir material publicitario o comercial (no institucional), así como distribución de cadenas de correos.
8) Instalar software en la plataforma tecnológica de las instituciones y entidades del Sector Defensa, cuyo uso no esté autorizado por la Oficina de Tecnología o quien haga sus veces, atentando contra las leyes de derechos de autor o propiedad intelectual.
9) Destruir la documentación institucional, sin seguir los parámetros y normatividad vigente establecida para el proceso de gestión documental.
10) Descuidar información clasificada de las instituciones y entidades del Sector Defensa, sin las medidas apropiadas de seguridad que garanticen su protección.
11) Enviar información no pública por correo físico, copia impresa o electrónica sin la debida autorización y/o sin la utilización de los protocolos establecidos para la divulgación.
12) Almacenar y mantener información clasificada en dispositivo de almacenamiento de cualquier tipo que no sean de propiedad de las respectivas instituciones y entidades del Sector Defensa.
13) Conectar computadores portátiles u otros dispositivos electrónicos personales, a la red de datos de las instituciones y entidades del Sector Defensa, sin la debida autorización.
14) Ingresar a la red de datos de las instituciones y entidades del Sector Defensa, por cualquier servicio de acceso remoto, sin la autorización de la oficina de tecnología o la que haga sus veces.
15) Usar servicios de internet en los equipos de la institución, diferente al provisto por la oficina de tecnología o la que haga sus veces.
16) Promover o mantener actividades personales utilizando los recursos tecnológicos de las instituciones y entidades del Sector Defensa, para beneficio personal.
17) Uso de la cuenta y contraseña de otro usuario o facilitar, prestar o permitir el uso de su cuenta personal a otro funcionario.
18) Descuidar dejando al alcance de personas no autorizadas los dispositivos portátiles, móviles y de almacenamiento removibles, entregados para actividades propias del cumplimiento de sus funciones.
19) Retirar de las instalaciones de las instituciones y entidades del Sector Defensa, computadores de escritorio, portátiles e información clasificada física o digital sin autorización, o abandonarla en lugares públicos o de fácil acceso.
20) Entregar, enseñar o divulgar información clasificada de las instituciones y entidades del Sector Defensa personas o entidades no autorizadas.
21) Llevar a cabo actividades ilegales, o intentar acceso no autorizado a la plataforma tecnológica de las instituciones y entidades del Sector Defensa o de terceras partes.

22) Ejecutar cualquier acción que difame, afecte la reputación o imagen de las instituciones y entidades del Sector Defensa, o de alguno de sus funcionarios, utilizando para ello la plataforma tecnológica.
23) Realizar cambios no autorizados en la plataforma tecnológica de las instituciones y entidades del Sector Defensa.
24) Otorgar privilegios de acceso a los activos de información a funcionarios o terceros no autorizados.
25) Ejecutar acciones para eludir y/o modificar los controles establecidos en la presente directiva.
26) Realizar cualquier otra acción que contravenga disposiciones constitucionales, legales o institucionales.

La realización de alguna de estas prácticas u otras que afecten la seguridad de la información, acarrearán medidas administrativas, acciones disciplinarias y/o penales a que haya lugar, de acuerdo con los procedimientos establecidos para cada caso

F. NO REPUDIO

El Comando General de las Fuerzas Militares en cumplimiento de la política de seguridad y privacidad de la información, comprende la capacidad de no repudió con el fin de que los usuarios evite haber realizado alguna acción que vaya en contra de la normas, decretos y Leyes, establece a través de sus organización las normas de trazabilidad, retención, auditoria e intercambio electrónico de información

G. PRIVACIDAD Y CONFIDENCIALIDAD

La política de confidencialidad, debe contener un compromiso o acuerdo de confidencialidad, por medio del cual todo funcionario, contratista y/o tercero vinculado a la Entidad, deberá firmar un compromiso de no divulgar la información interna y externa que conozca de la Entidad, así

como la relacionada con las funciones que desempeña en la misma. La firma del acuerdo implica que la información conocida por todo funcionario, contratista y/o tercero, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización. La política deberá indicar desde cuando se firma el acuerdo de confidencialidad, así como la vigencia del mismo

Cuando se habla de datos personales se hace referencia a toda aquella información asociada a una persona que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, datos financieros, entre otros.

Los datos personales conforman la información necesaria para que una persona pueda interactuar con otras o con una o más empresas y/o entidades para que sea plenamente individualizada del resto de la sociedad, haciendo posible la generación de flujos de información que contribuyen con el crecimiento económico y el mejoramiento de bienes y servicios.

1. Ámbito de Aplicación.

   La aplicación de la Política de Tratamiento de Datos Personales por parte del Comando General de las Fuerzas Militares y las entidades adscritas y vinculadas será de estricto cumplimiento por parte de todos los funcionarios.

   En este sentido, el Comando General de las Fuerzas Militares, en cumplimiento a sus objetivos institucionales y su compromiso con la protección de los derechos de las personas y las empresas de resguardar la confidencialidad de sus datos, como lo expresa la Ley 1581 de 2012 y el Decreto 1377 de 2013, incorpora en el presente plan los lineamientos mínimos para la recolección, manejo, tratamiento de información y protección de los datos personales, De igual manera, busca unificar los criterios relacionados con la definición de los "términos de privacidad y condiciones de uso" de los diferentes sitios Web, medios electrónicos y servicios digitales habilitados y utilizados para la recolección de datos personales.

   La declaración de aplicabilidad menciona los controles existentes al momento de definir el Sistema de Gestión de Seguridad de la Información y realizar el análisis de riesgos, así como los controles y objetivos de control que han sido seleccionados con base en el análisis y evaluación de riesgos, en los requerimientos de seguridad identificados y por ende, en las definiciones dadas en el plan de tratamiento del riesgo. Estos controles están basados en los controles definidos en la norma ISO/IEC 27001. La declaración de aplicabilidad debe ser documentada y actúa las entidades que conforman el Comando General y sus Unidades.

2. Excepción al ámbito de aplicación de las políticas de tratamiento de datos personales.

   a. En la aplicación de la Política de Tratamiento de Datos Personales deberán observarse las excepciones del régimen de protección de datos personales, según las cuales, el ámbito de la Ley 1581 de 2012 no será aplicable a:

1) Los archivos y las bases de datos pertenecientes al ámbito personal o doméstico.
2) Los que tienen por finalidad la seguridad y la defensa nacional, la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.
3) Los que tengan como fin y contengan información de inteligencia y contrainteligencia.
4) Los de información periodística y otros contenidos editoriales.
5) Los regulados por la Ley 1266 de 2008 (información financiera y crediticia, comercial, de servicios y proveniente de terceros países)
6) Los regulados por la Ley 79 de 1993 (sobre censos de población y vivienda).

Teniendo en cuenta lo anterior, mediante la Ley 1581 de 2012 y el Decreto 1377 de 2013 el Gobierno Nacional expidió el marco general de la protección de los datos personales en Colombia estableciendo las normas para la protección del habeas data, otorgando a todas las personas que figuren registradas en una base de datos el derecho a conocer, actualizar y rectificar dichos registros, así como las transferencias de datos personales y la responsabilidad demostrada frente al tratamiento de datos personales.

Por otra parte, el Ministerio de Defensa Nacional emitió en el año 2014 la Directiva Permanente DIR2014-18: Políticas de Seguridad de la Información para el Sector Defensa, mediante la cual se establecen los criterios y comportamientos sobre los activos de información que permitan preservar la confidencialidad, integridad y disponibilidad de la información en el Sector Defensa. Allí se imparten instrucciones precisas a las unidades ejecutoras/dependencias, entidades adscritas y vinculadas y dependencias internas de estas, encaminadas a gestionar adecuadamente la seguridad de la información, de los sistemas informáticos y de los ambientes tecnológicos.

En cuanto al tratamiento de datos personales deberán tenerse en cuenta los lineamientos precisos de la Directiva Permanente DIR2014-18 y sus modificaciones, en particular lo relacionado con:

1) Implementación de los controles de seguridad requeridos para todos los sistemas de información e infraestructura tecnológica por parte de las oficinas de tecnología.
2) Inclusión de los temas relacionados con seguridad de la información y tratamiento de datos personales en los programas de inducción y re inducción.
3) Cumplimiento de instrucciones generales sobre Gestión de Terceros, Gestión y Uso de Activos de Información, Acuerdos de Intercambio de Información y Software, Clasificación de la Información, Copias de Respaldo y Gestión de Medios Removibles.

Los funcionarios deberán acogerse a las inhabilidades, impedimentos, incompatibilidades y conflicto de intereses contemplados en la Ley 734 de 2002 (Código Disciplinario Único, título IV, capítulo cuarto) para el tratamiento de datos personales. Así mismo, los contemplados en la Ley 1862 de 2017 (Normas de Conducta del Militar Colombiano y Código Disciplinario Militar).

Ante el ejercicio del derecho de acceso a la información pública en cabeza de la ciudadanía, se tendrá en cuenta lo anterior, y a su vez los criterios de armonización contemplados en la Ley 1712 de 2014 y sus reglamentaciones posteriores, en cada caso concreto que así lo requieran.

Se establece que el titular reconoce que la entrega de datos / información personal, la realiza de manera voluntaria y ante la solicitud de requerimientos específicos por

cualquiera de las unidades /dependencias del Comando General de las Fuerzas Militares para realizar un trámite, presentar una queja o reclamo, o para acceder a los mecanismos interactivos y servicios digitales habilitados.

b. Aviso de privacidad

El aviso de privacidad es la comunicación verbal o escrita dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

El aviso de privacidad, como mínimo, deberá contener la siguiente información:

1) La identidad, domicilio y datos de contacto del responsable del tratamiento.
2) El tipo de tratamiento al cual serán sometidos los datos y la finalidad del mismo.
3) Los mecanismos generales dispuestos por el responsable para que el titular conozca la política de tratamiento de la información y los cambios sustanciales que se produzcan en ella.

c. Principios esenciales para el tratamiento de datos personales

Para el desarrollo y aplicación del tratamiento de datos personales registrados en las bases de datos y archivos se observarán los principios rectores establecidos en el artículo 4° de la Ley 1581 de 2012 y de la Ley 1712 de 2014, los cuales serán objeto de aplicación de criterios de armonización, ante la duda de su aplicabilidad o conflicto entre los mismos, en el caso concreto.

1) Principio de legalidad: El tratamiento debe sujetarse a lo establecido en la ley 1581 de 2012 y demás disposiciones normativas que se desarrollen.
2) Principio de finalidad: El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al titular.
3) Principio de libertad: El tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular en los casos que establezca la ley. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
4) Principio de veracidad o calidad: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. No se debe dar tratamiento de datos parciales, incompletos, fraccionados o que induzcan al error.
5) Principio de transparencia: En el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan. Los sujetos obligados están en el deber de proporcionar y facilitar el acceso a la información en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales o legales.
6) Principio de acceso y circulación restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la ley y la Constitución. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la ley.

7) Los datos personales, salvo la Información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente.
8) Principio de seguridad: La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, perdida, consulta, uso o acceso no autorizado o fraudulento.
9) Principio de confidencialidad: Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

d. Principios relacionados con el acceso a la información pública de las Unidades/dependencias del Comando General de las Fuerzas Militares adscritas y vinculadas.

1) Principio de buena fe: Al cumplir con las obligaciones derivadas del derecho de acceso a la información pública, lo harán con motivación honesta, leal y desprovista de cualquier intención dolosa o culposa.
2) Principio de facilitación: Deberán facilitar el ejercido del derecho de acceso a la información pública, excluyendo exigencias o requisitos que puedan obstruirlo o impedirlo.
3) Principio de no discriminación: Deberán entregar información a todas las personas que lo soliciten, en igualdad de condiciones, sin hacer distinciones arbitrarias y sin exigir expresión de causa o motivación para la solicitud.
4) Principio de gratuidad: El acceso a la información pública es gratuito y no se podrá cobrar valores adicionales al costo de reproducción de la información.
5) Principio de celeridad: Se propenderán por la agilidad en los trámites y la gestión administrativa para atender los requerimientos de información.
6) Principio de eficacia: Facilitarán el ejercicio de los derechos colectivos e individuales relacionados con el acceso a información pública mediante el establecimiento de resultados mínimos en relación con las responsabilidades que les atañen.
7) Principio de la calidad de la información.: Toda la información de interés público que sea producida, gestionada y difundida por todas y cada una de las unidades/dependencias del Comando General de las Fuerzas Militares, deberá ser oportuna, objetiva, veraz, completa, reutilizable, procesable y estar disponible en formatos accesibles para los solicitantes e interesados en ella, teniendo en cuenta los procedimientos de gestión documental PRODOPAC.
8) Principio de la divulgación proactiva de la información: El derecho de acceso a la información no radica únicamente en la obligación de dar respuesta a las peticiones de la sociedad, sino también en el deber de todas las unidades/dependencias del Comando General de las Fuerzas Militares entidades adscritas y vinculadas de promover y generar una cultura de transparencia, lo que conlleva la obligación de publicar y divulgar documentos y archivos que plasman la actividad estatal y de interés público, de forma rutinaria y proactiva, actualizada, accesible y comprensible, atendiendo a límites razonables del talento humano y recursos físicos y financieros.

e. Tratamiento de datos personales

La recolección y almacenamiento de datos personales en las bases de datos debe obedecer únicamente al ejercicio dé las funciones legales y misionales de los responsables del tratamiento de datos personales. En ese sentido se debe garantizar la protección de derechos como el habeas data, la privacidad, la intimidad, el buen nombre, la Imagen y la autonomía institucional, y a su vez el de acceso a la información; por tanto, el tratamiento de datos personales deberá realizarse cumpliendo con la normatividad legal colombiana vigente que establezca disposiciones para la protección de datos personales.

Así mismo se debe divulgar al personal uniformado de la Fuerza Pública, personal civil al servicio de las unidades/dependencias del Comando General de las Fuerzas Militares, personal no uniformado, personal vinculado a través de contratos de prestación de servicios y demás involucrados encargados del tratamiento, las obligaciones que tienen relación con el tratamiento de datos personales mediante campañas y actividades pedagógicas; y documentar el/los procedimientos relacionados con el tratamiento de datos personales, conforme a lo establecido en sus respectivos Sistemas de Gestión.

f. Responsables y encargados del tratamiento de datos personales

Cada una de las unidades /dependencias del Comando General de las Fuerzas Militares son responsables del tratamiento de datos personales registrados sus bases de datos personales en forma presencial en las sedes habilitadas para ello y de forma virtual a través de los diferentes mecanismos tecnológicos y servicios digitales (incluido el sitio Web).

Los encargados del tratamiento de los datos personales son el personal civil y uniformado al servicio del Comando General de las Fuerzas Militares y sus unidades adscritas y vinculadas, así como las personas naturales o jurídicas vinculadas a través de cualquier tipo de contratación, que en cumplimiento de sus funciones o del objeto contractual realicen operaciones sobre datos personales, tales como recolección, almacenamiento, uso, circulación o supresión. Lo anterior es extensible a estudiantes en prácticas que realicen o apoyen este tipo de funciones.

g. Derechos de los titulares de los datos personales

En atención a lo dispuesto en la normatividad vigente y aplicable en materia de protección de datos personales, el titular de los datos personales tiene los siguientes derechos:

1) Conocer, actualizar y rectificar sus datos personales ante el responsable del tratamiento de datos personales. Este derecho se podrá ejercer, entre otros, ante datos pardales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o que no haya sido autorizado por el titular.
2) Solicitar prueba de la autorización otorgada al responsable del tratamiento de datos personales, salvo en los casos expresamente exceptuados en la Ley.
3) Ser informado por responsable del tratamiento de datos personales, previa solicitud, respecto del uso que se le ha dado a sus datos personales.

4) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen.
5) Revocar la autorización y/o solicitar la supresión del dato, cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. Exceptuando los casos en que el titular tenga un deber legal o contractual de permanecer en la base de datos del responsable o encargado.

h. Autorización del titular

El responsable del tratamiento de datos personales tendrá como soporte de la autorización del titular de los datos personales un documento físico, electrónico, mensaje de datos, Internet, sitios web, o en cualquier otro formato que permita garantizar su posterior consulta, o mediante un mecanismo técnico o tecnológico idóneo que permita manifestar u obtener el consentimiento, mediante el cual se pueda concluir de manera inequívoca, que de no haberse surtido una conducta del titular, sus datos personales nunca hubieren sido capturados y almacenados en la base de datos. El medio para otorgar la autorización por parte del titular será puesto en su conocimiento, y a su disposición, con antelación y de manera previa al tratamiento de sus datos personales.

El responsable del tratamiento de datos personales adoptará las acciones tendientes y necesarias para mantener registros o mecanismos técnicos o tecnológicos idóneos de cuándo y cómo obtuvo autorización por parte de los titulares de datos personales para el tratamiento de los mismos. Para dar cumplimiento a lo anterior, se podrán establecer archivos físicos o repositorios electrónicos realizados de manera directa o a través de terceros contratados para tal fin.

i. Revocatoria de la autorización

Los titulares de los datos personales pueden revocar el consentimiento al tratamiento de los mismos en cualquier momento ante responsable del tratamiento de datos personales, siempre y cuando no lo impida una disposición legal o contractual. En caso de proceder la revocatoria de tipo parcial de la autorización para el tratamiento de datos personales para algunas finalidades, el responsable del tratamiento de datos personales podrá seguir utilizando los datos para las demás finalidades respecto de las cuales no proceda dicha revocatoria.

j. Tratamiento de datos sensibles

Los datos que afecten la intimidad del titular o cuyo uso indebido pueda generar su discriminación sólo pueden ser objeto de tratamiento, por parte de las unidades ejecutoras/dependencias y de las entidades adscritas y vinculadas al del Comando General de las Fuerzas Militares, en los siguientes casos:

1) Cuando el titular de la información manifieste su conformidad y dé su autorización, por cualquier medio que permita su conservación, para el tratamiento de sus datos sensibles.
2) Cuando el tratamiento se requiera para proteger la vida del titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, el representante legal en su calidad de responsable del tratamiento deberá otorgar su autorización.

3) Cuando el tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de un ente de control, fundación, ONG, asociación, o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea judicial, política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos reguladores por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin autorización del titular.
4) Cuando el tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho de un proceso judicial.
5) Cuando el tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

k. Protección de datos personales en Sistemas de Videovigilancia

Los Sistemas de Videovigilancia o cámaras de seguridad implementadas con la finalidad de garantizar la seguridad de bienes o personas en un lugar determinado, mediante las cuales se realicen tareas de monitoreo y observación, implican la recopilación de imágenes de personas, es decir, de datos personales de acuerdo con la definición contenida en el literal c) del artículo 3 de la Ley 1581 de 2012.

En consecuencia, los responsables del tratamiento de datos personales deben observar los principios establecidos en la mencionada norma, y adoptados en la presente Directiva, así como las demás disposiciones contenidas en el Régimen General de Protección de Datos Personales, y en particular las siguientes.

1) Implementar Sistemas de Videovigilancia sólo cuando sea necesario para el cumplimiento de la finalidad propuesta, respetando la dignidad y demás derechos fundamentales de las personas.
2) Informar a los Titulares sobre la recolección de imágenes a través de sistemas de Videovigilancia, así como la finalidad de dicha recolección y el tratamiento del que serán objeto las imágenes recolectadas para ello.
3) Determinar el tiempo de conservación de las imágenes, conforme a la finalidad establecida para su captura y conservarlas sólo por ese tiempo.
4) Inscribir la base de datos que almacena las imágenes en el Registro Nacional de Bases de Datos - RNBD. No será necesaria la inscripción cuando el Tratamiento consista sólo en la reproducción o emisión de imágenes en tiempo real, sin perjuicio del cumplimiento de las demás disposiciones del Régimen General de Protección de Datos Personales.
5) Suscribir acuerdos de confidencialidad, e incluir cláusulas al respecto en los contratos en que aplique, con el personal que accederá a los Sistemas de Videovigilancia.
6) Cuando los Sistemas de Videovigilancia sean dispuestos en lugares destinados para el registro de acceso a las instalaciones de las unidades ejecutoras/dependencias del Ministerio de Defensa Nacional, de la Policía Nacional y las entidades adscritas o vinculadas al Ministerio de Defensa Nacional, o en zonas de éstas instalaciones destinadas para la atención al público, así como a unidades militares y policiales, en todos los casos, mediante el aviso de privacidad, se debe informar sobre ello a los titulares de datos personales indicando que con su ingreso conocen y autorizan el almacenamiento y posterior tratamiento de las imágenes grabadas.

Toda vez que garantizar la seguridad en entornos públicos es tarea que corresponde de forma exclusiva al Estado, las unidades de la Fuerzas Militares y de la Policía Nacional se encuentran legitimadas para operar Sistemas de Videovigilancia en la vía pública.

l. Garantías de derecho de acceso y consultas

Los Titulares de la información podrán acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento, previa acreditación de su identidad o de su representante. La información solicitada por el titular podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el titular. Los responsables del tratamiento de datos personales deberán poner a disposición del titular de la información, mecanismos gratuitos y de fácil acceso para presentar la solicitud de sus datos, de supresión de los mismos o la revocatoria de la autorización.

En el caso de consultas y solicitudes de información o datos personales que provengan de terceros y/o no titulares de lo solicitado, se tendrá en cuenta la aplicabilidad por parte del responsable del tratamiento las excepciones constitucionales y legales que aplican en la materia, y de los resultados que arrojen los juicios de proporcionalidad y razonabilidad que permitan conceder o negar el derecho de acceso a lo solicitado, cuando la sensibilidad del caso estrictamente así lo requiera.

Los responsables del tratamiento de datos personales garantizarán el derecho de consulta, suministrando a los titulares, o a través de un tercero debidamente autorizado, toda la información contenida en el registro individual o que esté vinculada con la identificación del titular.

Los titulares, podrán consultar sus datos de manera directa. En consecuencia, con respecto a la atención de solicitudes de consulta de datos personales los responsables del tratamiento de datos personales garantizarán:

1) Habilitar medios de comunicación electrónica u otros que considere pertinentes.
2) Establecer formularios, sistemas y otros métodos simplificados, que deben ser informados en el aviso de privacidad.
3) Acceder a los servicios de atención al cliente o de reclamaciones que tiene en operación.

m. Reclamos

El titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando advierten el presunto incumplimiento de cualquiera de los deberes contenidos en la normatividad vigente en la materia o en la presente política, podrán presentar un reclamo ante el responsable del tratamiento o el encargado del tratamiento, canalizándola y remitiéndola a través de la dependencia designada para tal fin, la cual ejercerá la función de protección de datos personales, conforme a lo que se ¿establezca en el respectivo manual de procedimientos.

El responsable del tratamiento de datos personales actualizará, rectificará o suprimirá los datos personales a solicitud del titular para corregir información parcial, inexacta, incompleta, fraccionada que induzca al error o aquella que haya sido tratada previa a la vigencia de la ley y que no tenga autorización o sea prohibida.

Para ello, tienen plena libertad de habilitar mecanismos que le faciliten el ejercicio de este derecho, siempre y cuando éstos beneficien al titular. En consecuencia, se podrán habilitar medios electrónicos u otros que considere pertinentes; igualmente podrá establecer formularios, sistemas y otros métodos simplificados, que deben ser informados en el aviso de privacidad y que se pondrán a disposición de los interesados en la página web, servicios digitales habilitados y demás medios electrónicos que consideren pertinentes.

En el evento en que el titular considere que se dio un uso contrario al autorizado y a las leyes aplicables, podrá hacer uso de sus derechos a través de mecanismos habilitados para ello, para lo cual el responsable del tratamiento de datos personales publicará la información suficiente y necesaria para realizar el contacto en su sede física o a través del correo electrónico u otros medios electrónicos.

n. Seguridad de la información y medidas de seguridad

En desarrollo del principio de seguridad establecido en la normatividad vigente, y observando particularmente lo establecido en la Directiva Ministerial Permanente DIR2014-18 "Políticas de Seguridad de la Información para el Sector Defensa" y sus modificaciones, el responsable del tratamiento de datos personales adoptará las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; efectuará un correcto tratamiento de los datos personales contenidos en sus bases de datos, evitando el acceso no autorizado a terceros que puedan conocer, vulnerar, modificar, divulgar y/o destruir la información que se encuentra almacenada. Para esto aplicará los respectivos protocolos de seguridad y acceso a los sistemas de información, almacenamiento, procesamiento y medidas físicas de control *de riesgos de seguridad.*

Así mismo implementará las mejoras a los mecanismos de seguridad, así como la aplicación de instructivos y desarrollo de actividades de seguimiento a nivel interno para garantizar el correcto funcionamiento de los esquemas de seguridad técnica; sin embargo a pesar de las medidas adoptadas , ninguna de los responsable de tratamiento de datos personales se responsabilizará por cualquier consecuencia derivada del ingreso indebido o fraudulento por parte de terceros a las bases de datos y/o por falla técnica en el funcionario.

Los datos personales que no sean público serán tratados por el respectivo responsable del tratamiento de datos personales como confidenciales, aun cuando la relación contractual o el vínculo entre el titular del dato personal y la institución haya finalizado a la terminación del dicho vinculo, tales datos personales deberá continuar siendo tratados de acuerdo con lo dispuesto en el manual de procedimientos de gestión documental (PRODOPAC) vigente. .

El responsable del tratamiento de datos personales se reserva, en los eventos contemplados en la ley y en su normatividad interna, la facultad de mantener y catalogar *determinada información que repose en sus bases o bancos de datos, como confidencial* de acuerdo a las normas vigentes y reglamentos, todo lo anterior en conformidad con el derecho fundamental y constitucional y principalmente de la autonomía administrativa.

Los responsables de tratamiento de datos personales deben evaluar la pertenencia de anonimizar o seudonimizar los actos administrativos y/o documentos de carácter público que contenga datos personales, para su publicación.

Los responsables del tratamiento de datos personales no publicarán datos personales a través de Internet, medio digitales u otro medio masivos de comunicación, a menos que se trate de información pública o que se establezcan medidas técnicas que permita controlar el acceso y restringirlo sólo a las personas autorizadas por la ley o por el titular.

La información personal proporcionada por el titular, mediante aplicaciones móviles, sitios web, servicios digitales u/o mecanismos electrónicos, deberá estar asegurada por una clave de acceso que sólo el titular conoce, por lo tanto él es el único responsable de mantener en secreto su clave. Debido a que ninguna transmisión por internet es absolutamente segura ni puede garantizarse dicho extremo, el usuario acepta y asume los posibles riesgos asociados, y que se puedan materializar al transmitir información por Internet.

o. Intercambio y suministro de datos personales a terceros.

Los departamentos /dependencias y unidades vinculadas y adscritas al Comando General de las Fuerzas Militares suministrará e intercambiara entre sí y con terceros que le provean servicios o con quien tenga algún tipo de relación contractual o de cooperación , datos personales con el fin de:

1) Usar los datos del usuario para dar repuestas a sus peticiones, quejas, reclamos o requerimientos.
2) Manejar y administrar base de datos sectoriales.
3) Dar respuestas a organismos de control
4) Realizar estudios de seguridad

Cuando las dependencias/unidades adscritas y vinculadas del Comando General de las Fuerzas Militares intercambien información de datos personales entre sí o con terceros, por solicitud o por la ejecución de procesos previos y formalmente establecidos, deberá dar el mismo tratamiento de confidencialidad y seguridad que se le proporciona a la información producida.

En este sentido, en la sección de misiones particulares de la presente directiva, se instruirá quienes conforman el sector defensa sobre su calidad de responsables del tratamiento de los datos por ellos recaudados y las responsabilidades de privadas de ello.

p. Transferencia y transmisión de datos personales e información personal.

Las dependencias/unidades adscritas y vinculadas del Comando General de las Fuerzas Militares podrá transferir información de datos personales, sin que medie autorización expresa del titular, a las autoridades gubernamentales, administrativas, de impuestos, organismos de investigación y autoridades judiciales, cuando la solicite en ejercicio de sus funciones y atendiendo a las garantías, constitucionales y legales y al contenido de las presente directiva permanente.

La transferencia y transmisión internacional de datos personales, para su almacenamiento permanente y posterior tratamiento, sólo se realizará a países que proporcionen niveles adecuados de protección de datos, de acuerdo a los estándares y previa declaración de conformidad por parte de la Superintendencia de Industria y Comercio, quien verificará la viabilidad de la operación.

q. Derechos de los niños, niñas y adolescentes, víctimas de violencia sexual y víctimas del conflicto armado.

El tratamiento de datos personales de los niños, niñas y adolescentes, víctimas de violencia sexual y víctimas del conflicto armado, se asegurará el respecto a los derechos prevalentes de este grupo., estableciendo que debe que quedar pro escrito el tratamiento de datos salvo aquellos que sean de naturaleza pública; por tanto los responsables del tratamiento de datos personales velará por el tratamiento adecuado de los mismos, respetando el interés superior de aquellos y asegurando la protección de sus derechos fundamentales.

Así mismo se procederá del tratamiento de datos personales referente a las víctimas de violencia sexual en los términos del artículo 13 de la Ley 1719 de 2014, y de las víctimas del conflicto armado en los términos de los artículos 23, 29 y 156 de la Ley 1448 de 2011, por lo que dicho tratamiento en estos casos, se realizará mediante la debida valoración de los mismos.

Cuando se refiera al tratamiento de imágenes de niños, niñas y adolescentes, se debe respetar los derechos prevalentes de los mismos y sólo se podrá realizar cuando (i) responda y respete su interés superior, y (ii) asegure el respeto de sus derechos fundamentales. En todos los casos, los responsables y encargados que utilicen Sistemas de Videovigilancia que involucren el Tratamiento de imágenes de niños, niñas y/o adolescentes deben contar con la autorización de los padres o representantes legales de los menores y con la aquiescencia de estos, teniendo en cuenta su madurez, autonomía y capacidad para entender el asunto; así mismo, se debe Informar a los padres o representantes legales acerca de la finalidad y el tratamiento al cual serán sometidos los datos personales de los menores, así como los derechos que les asisten.

r. Responsabilidad demostrada frente al tratamiento de datos personales.

Los Comandante, Directores de Departamentos, Dependencias del Comando General de las Fuerzas Militares, Gerentes de las entidades adscritas del Comando General como cabezas máximas, son los responsables del tratamiento de datos personales y, en consecuencia, se encuentran obligados frente a la implementación de la Responsabilidad Demostrada.

En lo que corresponde a la organización del Comando General de la Fuerzas Militares, la responsabilidad del tratamiento de datos personales y la implementación de la Responsabilidad Demostrada, será delega por el Departamento Conjunto de Comunicaciones CGDJ6

El principio fundamental de responsabilidad demostrada exige que una entidad que recoge y hace tratamiento de datos personales debe ser responsable del cumplimiento efectivo de las medidas que implementen los principios de privacidad y protección de datos. En ese sentido, los Responsables del Tratamiento deben contar con un Programa

Integral de Gestión de Datos Personales (PIGDP) y estar preparados para demostrarle a la autoridad la implementación efectiva de esas medidas en la organización. La responsabilidad demostrada es una obligación en cabeza de los Responsables del Tratamiento (Decreto 1377/2013, Art. 26).

De acuerdo al Decreto 1377 de 2013 las unidades ejecutoras/dependencias del Ministerio de Defensa Nacional, la Policía Nacional y las entidades adscritas y vinculadas al Ministerio de Defensa Nacional deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado las medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y el Decreto 1377 de 2013, en las que sea evidente la naturaleza de los datos personales objeto del tratamiento y el tipo de tratamiento del que han sido objeto. Así mismo, los riesgos potenciales que el referido tratamiento podría causar sobre los derechos de los titulares.

Así las cosas, en respuesta a solicitud de la Superintendencia de Industria y Comercio, deberán suministrar la descripción de los procedimientos usados para la recolección de los datos personales, la descripción de las finalidades para las cuales esta información es recolectada, explicación sobre la relevancia de los datos personales en cada caso, y evidencia sobre la implementación efectiva de las medidas de seguridad adoptadas para la protección de los datos personales.

s. Denegación o rechazo del Derecho de Acceso a la Información Pública por Clasificación o Reserva

El acto de respuesta del sujeto obligado que deniegue o rechace una solicitud de acceso a información pública por razón de clasificación o reserva, deberá seguir las directrices señaladas en la Ley.

La respuesta a la solicitud deberá ser gratuita o sujeta a un costo que no supere el valor de la reproducción y envío de la misma al solicitante. Se preferirá, cuando sea posible, según los sujetos pasivo y activo, la respuesta por vía electrónica, con el consentimiento del solicitante".

Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito, siempre que el acceso pudiere causar un daño a los siguientes derechos:

1) El derecho de toda persona a la intimidad, bajo las limitaciones propias que impone la condición de servidor público, en concordancia con lo estipulado.

2) El derecho de toda persona a la vida, la salud o la seguridad.
3) Los secretos comerciales, industriales y profesionales.

Parágrafo. "Estas excepciones tienen una duración ilimitada y no deberán aplicarse cuando la persona natural o jurídica ha consentido en la revelación de sus datos personales o privados o bien cuando es claro que la información fue entregada como parte de aquella información que debe estar bajo el régimen de publicidad aplicable".

t. Divulgación parcial y otras reglas.

En aquellas circunstancias en que la totalidad de la información contenida en un documento no esté protegida por una excepción contenida en la presente ley, debe hacerse una versión pública que mantenga la reserva únicamente de la parte indispensable. La información pública que no cae en ningún supuesto de excepción deberá ser entregada a la parte solicitante, así como ser de conocimiento público. La reserva de acceso a la información opera respecto del contenido de un documento público pero no de su existencia.

Ninguna autoridad pública puede negarse a indicar si un documento obra o no en su poder o negar la divulgación de un documento, salvo que el daño causado al interés protegido sea mayor al interés público de obtener acceso a la información.

Las excepciones de acceso a la información contenidas en la ley no aplican en casos de violación de derechos humanos o delitos de lesa humanidad, y en todo caso deberán protegerse los derechos de las víctimas de dichas violaciones".

H. *INTEGRIDAD*

La política de integridad debe ser conocida y aceptada por todos los funcionarios, contratistas y/o terceros que hagan parte de la Entidad, la cual se refiere al manejo íntegro e integral de la información tanto interna como externa, conocida o administradas por los mismos.

De esta manera, toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información.

En el caso de vinculación contractual, el Compromiso de administración y manejo integro e integral de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de Cláusula de integridad de la información. La política de integridad, deberá establecer asimismo la vigencia de la misma acorde al tipo de vinculación del personal al cual aplica el cumplimiento.

I. DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN.

El Comando General de las Fuerzas Militares contará con un plan de continuidad del negocio el cual estará a cargo del Oficial de Seguridad y Privacidad de la Información con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales de la Entidad, ante el evento de un incidente de seguridad de la información. La política de disponibilidad debe incluir como mínimo los siguientes aspectos:

1. Niveles de disponibilidad: Esta política debe velar por el cumplimiento de los niveles de disponibilidad de servicios e información acordados con clientes, proveedores y/o terceros

en función de las necesidades de la Entidad, los acuerdos de nivel de servicios ofrecidos y evaluaciones de riesgos.

2. Planes de recuperación: La política debe incluir los planes de recuperación que incluyan las necesidades de disponibilidad del negocio.
3. Interrupciones: La política debe velar por la gestión de interrupciones de mantenimiento de los servicios que afecten la disponibilidad de este.
4. Acuerdos de Nivel de servicio: Tener en cuenta los acuerdos de niveles de servicios (ANS) en las interrupciones del servicio.
5. Segregación de ambientes: Esta política debe establecer la segregación de ambientes para minimizar los riesgos de puesta en funcionamiento de cambios y nuevos desarrollos con el fin de minimizar el impacto de la indisponibilidad del servicio durante las fases de desarrollo, pruebas y producción.
6. Gestión de Cambios: La política debe incluir gestión de cambios para que los pasos a producción afecten mínimamente la disponibilidad y se realicen bajo condiciones controladas.

J. REGISTRO Y AUDITORÍA.

1. Responsabilidad: La Inspección General y/o el Departamento Conjunto de Planificación Transformación CGDJ5 del Comando General de las Fuerzas Militares tendrá la responsabilidad realizar auditorías a los procesos del Sistema de Gestión de Seguridad de la Información, una vez Implementado, como mínimo una vez al año.

2. Almacenamiento de Registros: La administración debe incluir el almacenamiento de los registros de las copias de seguridad en las bases de datos que está bajo la responsabilidad del Departamento Conjunto de Comunicaciones CGDJ6 correspondiente y el correcto funcionamiento de las mismas, los registros de auditoria debe incluir toda la información, registro y monitoreo de seguridad.

3. Normatividad: La auditoría debe velar porque las mismas sean realizadas acorde a la normatividad y requerimiento legales aplicables a la naturaleza del Comando General de las Fuerzas Militares.

4. Garantía de Cumplimiento: La auditoría debe garantizar la evaluación de los controles, la eficiencia de los sistemas de cumplimiento de las políticas y procedimientos del Comando General de las Fuerzas Militares; así como recomendar las deficiencias detectadas.

5. Periodicidad: La auditoría debe determinar la revisión periódica de los niveles de riesgos a los cuales está expuestas el Comando General de las Fuerzas Militares, lo cual se logra a través de auditorías periódicas alineadas a los objetivos estratégicos y gestión de procesos.

K. CAPACITACION Y SENSIBILIZACION EN SEGURIDAD DE LA INFORMACION.

1. El Departamento Conjunto de Educación Militar CGDJ7, liderará la Capacitación y Sensibilización incluyendo dentro de los programas de capacitación temas relacionados con la seguridad de la información cuya finalidad es disminuir las vulnerabilidades y amansas relacionadas con el recurso humano.

   a. Se deberá destinar recursos necesarios para el desarrollo de los Programas de Seguridad y Privacidad de las Información.
   b. Se deberá entrenar a los Gestores Documentales, Personal de la Dirección de Gestión Documental DIGED, el Personal de la Dirección de las Tecnología de las Información, Personal de la Dirección de Contrainteligencia Conjunta, Personal de la Dirección de Seguridad, Personal de Dirección de Personal del Comando - DIPEC en los temas relacionados con las Seguridad y Privacidad de las Información
   c. El oficial de las Tecnologías de la Información realizara la sensibilización a todo el personal del Comando General de las Fuerzas Militares en la Seguridad y Privacidad de las Información.
   d. Es obligación de todo el personal del Comando General asistir a los eventos de capacitación y sensibilización de acuerdo a la distribución de cupos.
   e. Es responsabilidad del Oficial de Seguridad y Privacidad de las Información hacer las revisiones periódicas de los resultados de las capacitaciones teniendo en cuenta la permanencia del personal de Oficiales y Suboficiales para el manejo de los procesos.
   f. El Oficial de Seguridad y Privacidad de las Información llevará los registros de los planes y programas desarrollados del sistema de seguridad y privacidad de la información.
   g. Todos los funcionarios del Comando General deberá llenar el Acta de Compromiso de Reserva de las Información formato que será suministrado por el Departamento Conjunto de Inteligencia de Contra Inteligencia CGDJ2.

2. Oficinas de Telemática, Informática, Sistemas o de Tecnología

   a. Promover el cumplimiento, por parte del personal bajo su responsabilidad, de las políticas de seguridad de la información.
   b. Implementar y administrar las herramientas tecnológicas para el cumplimiento de las políticas de seguridad de la información.
   c. Registrar y mantener la información requerida para auditar y evaluar la ejecución de los controles específicos de seguridad de la información.
   d. Incluir los controles de seguridad de la información en el diseño, desarrollo, instalación y mantenimiento de las aplicaciones bajo su responsabilidad.
   e. Implementar y administrar los controles de seguridad sobre la información y conexiones de las redes de datos bajo su administración.
   f. Definir e implementar la estrategia de concientización y capacitación en seguridad de la información para los funcionados y terceros, cuando aplique.
   g. Custodiar la información y los medios de almacenamiento bajo su responsabilidad.
   h. Garantizar la implementación de las recomendaciones generadas en los análisis de vulnerabilidades.

i. Definir, mantener y controlar la lista actualizada de software y aplicaciones autorizadas; así mismo, realizar el control y verificación de cumplimiento del licenciamiento software y aplicaciones asociadas.
j. Monitorear y evaluar los procesos o actividades sobre las plataformas tecnológicas, delegados en terceros.
k. Establecer, verificar, monitorear y validar los procedimientos de continuidad y de contingencias para cada una de las plataformas tecnológicas criticas bajo su responsabilidad.
l. Establecer, documentar y actualizar los procedimientos de seguridad de la información que apliquen para la plataforma de tecnologías de información administrada por esta oficina.
m. Gestionar los incidentes de seguridad de la información que se presenten.
n. Realizar análisis de vulnerabilidades a la plataforma tecnológica con el fin de generar recomendaciones.

3. Unidades de Ciberseguridad y Ciberdefensa (CCOCI)

a. Comando Conjunto Cibernética (CCOCI): Desarrollar estrategias, programas, proyectos y demás actividades requeridas para garantizar la Ciberdefensa de los activos críticos de las instituciones y entidades del Sector Defensa del Comando General.
b. Coordinar temas de Ciberseguridad y Ciberdefensa y la protección de la infraestructura critica nacional con el Grupo de Respuestas a Emergencias Cibernéticas de Colombia (colCERT) a nivel del Ministerio de Defensa
c. Centro Cibemético Policial (CCP): Desarrollar estrategias, programas, proyectos y demás actividades requeridas en materia de investigación criminal contra los delitos que afectan la información y los datos.

4. Oficinas de personal o de talento humano.

Incluir en los programas de inducción y de re-inducción 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.

5. Departamento Conjunto de Inteligencia y Contrainteligencia - Unidades y/o secciones de Inteligencia de la Fuerzas o quien haga sus veces en las Instituciones y entidades definidas en el presente plan.

a. Elaborar y actualizar los estudios de credibilidad y confiabilidad, las actas de compromiso de reserva, las pruebas técnicas de confidencialidad y las tarjetas de autorización para manejo de documentación clasificada de los funcionarios y contratistas que laboran en los organismos de inteligencia y contrainteligencia de las Fuerzas Militares.
b. Desarrollar actividades de monitoreo del uso de los activos de información propios para prevenir el impacto de los riesgos derivados de la violación de la reserva legal y la pérdida de integridad, disponibilidad y confidencialidad de la información.
c. Supervisar el cumplimiento de los procedimientos y controles para evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de los organismos de inteligencia y contrainteligencia de las Fuerzas Militares.
d. Desarrollar las actividades para el soporte del Centro de Protección de Datos de Inteligencia de acuerdo a lo estipulado en la normatividad vigente.

e. Asignar los niveles de clasificación, seguridad y restricciones en la difusión a los productos que se envían a los receptores autorizados por la ley.
f. Elaborar y ejecutar planes de capacitación sobre las políticas de seguridad de la información a los organismos de inteligencia y contrainteligencia de las unidades operativas y tácticas de las Fuerzas Militares.
g. Realizar monitoreo del uso de los activos de información para prevenir el impacto de los riesgos derivados de pérdida de integridad, disponibilidad y confidencialidad de la información.
h. Supervisar el cumplimiento de los procedimientos y controles para evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de las instituciones y entidades que la conforman en las diferentes unidades de las Fuerzas Militares.

6. Propietarios de la Información en cada uno de los procesos.

a. Clasificar los activos de información bajo su responsabilidad de acuerdo con los requerimientos de confidencialidad, integridad y disponibilidad, así como verificar que se les proporcione un nivel adecuado de protección, de conformidad con los estándares, políticas y procedimientos de seguridad de la información.
b. Definir los acuerdos de niveles de servicio para recuperar sus activos de información y sistemas críticos e identificar los impactos en caso de una interrupción extendida.
c. Definir los requerimientos de continuidad y de recuperación en caso de desastre.
d. Coordinar la realización de un análisis de riesgos como mínimo una vez al año, para determinar el grado de exposición a las amenazas vigentes y confirmar los requerimientos de confidencialidad, integridad y disponibilidad relacionados con sus activos de Información.
e. Comunicar sus requerimientos de seguridad de información al área correspondiente.
f. Determinar y autorizar todos los privilegios de acceso a sus activos de información.
g. Comunicas al área correspondiente sus requerimientos en capacitación sobre seguridad de información.
h. Revisar los registros y reportes de auditoria para asegurar el cumplimiento con las restricciones de seguridad para sus activos de información. Estas revisiones podrán realizarse en coordinación con el custodio del activo, verificando los resultados de las revisiones y reportando cualquier situación que involucre un incumplimiento o violación a la seguridad de Información, de acuerdo con el procedimiento de Gestión de Incidentes de Seguridad.
i. Participar en la resolución 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.

7. Dirección de Seguridad de las Fuerzas Militares.

Estará bajo la responsabilidad de la Dirección de Seguridad las siguientes actividades Y establecer los protocolos necesarios en coordinación con el Departamento Conjunto de Inteligencia y Contrainteligencia.

a. Seguridad Física:

1) Protección de las Instalaciones del Comando General de las Fuerzas Militares.
2) Estudios de seguridad de las instalaciones
3) Inspecciones de seguridad
4) Pruebas de vulnerabilidad
5) Coordinar la revisión de prevención electrónica
6) Establecer los protocolos para el acceso a las áreas restringidas
7) Realizar los planes de seguridad y prevención

b. Protección de Personas:

1) Evaluación de Riesgos.
2) Estudios de Rutas.
3) Estudios de Seguridad de Personal (ESP).
4) Estudio de Credibilidad y Confiabilidad.
5) Exámenes Técnicos Psicológicos de Polígrafo.
6) Llevar la base de datos del personal que tiene acceso a las instalaciones
7) Realizar los ficheros del personal de funcionarios personales y de vehículos

VI. DIRECTRICES GENERALES PARA LA PUBLICACIÓN DE INFORMACIÓN PÚBLICA

A. Estándares para publicar la información: El Ministerio de Tecnologías de la Información y las Comunicaciones a través de la estrategia de Gobierno en Línea expedirá los lineamientos que deben atender los sujetos obligados para cumplir con la publicación y divulgación de la información señalada en la Ley, con el objeto de que sean dispuestos de manera estandarizada.

B. Publicación de información en sección particular del sitio web oficial, deben publicar en la página principal de su sitio web oficial, en una sección particular identificada con el nombre de "Transparencia y acceso a información pública", la siguiente información:

1. El Registro de Activos de Información.
2. El Índice de Información Clasificada y Reservada.
3. El Esquema de Publicación de Información.
4. El Programa de Gestión Documental.
5. Las Tablas de Retención Documental.
6. El informe de solicitudes de acceso a la información
7. Los costos de reproducción de la información pública, con su respectiva motivación.

Directorio de Información de servidores públicos, empleados y contratistas, los sujetos obligados, de conformidad con las condiciones establecidas en la ley, deben publicar de forma proactiva un directorio de sus servidores públicos, empleados, y personas naturales vinculadas mediante contrato de prestación de servicios.

Para las entidades u organismos públicos, el requisito se entenderá cumplido con publicación de la información que contiene el directorio en el Sistema de Gestión del Empleo Público (SIGEP).

La publicación de la información de los contratos de prestación de servicios en el Sistema de Gestión del Empleo Público (SIGEP) no releva a los sujetos obligados que contratan con recursos públicos de la obligación de publicar la actividad contractual de tales contratos en el Sistema Electrónico para la Contratación Pública (SECOP).

a. Publicación de los trámites y servicios que se adelantan ante los sujetos obligados. Los sujetos obligados deben publicar en su sitio web oficial los trámites que se adelanten ante los mismos, señalando la norma que los sustenta, procedimientos, costos, formatos y formularios requeridos.

b. Publicación de la información contractual, el sistema de información del Estado en el cual los sujetos obligados que contratan con cargo a recursos públicos deben cumplir la obligación de publicar la información de su gestión contractual es el Sistema Electrónico para la Contratación Pública (SECOP).

   Los sujetos obligados que contratan con recursos públicos y recursos privados, deben publicar la información de su gestión contractual con cargo a recursos públicos en el Sistema Electrónico para la Contratación Pública (SECOP).

c. Publicación de la ejecución de contratos, el sujeto obligado debe publicar las aprobaciones, autorizaciones, requerimientos o informes del supervisor o del interventor, que prueben la ejecución del contrato.

d. Publicación de procedimientos, lineamientos y políticas en materia de adquisición y compras. Para los sujetos obligados que contratan con cargo a recursos públicos, los procedimientos, lineamientos y políticas en materia de adquisición y compras son los previstos en el manual de contratación expedido conforme a las directrices señaladas por la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente-, el cual debe estar publicado en el sitio web oficial del sujeto obligado.

e. Publicación de Datos Abiertos para la publicación de datos abiertos, serán elaboradas por el Ministerio de Tecnologías de la Información y las Comunicaciones y publicadas en el Portal de Datos Abiertos del Estado colombiano o la herramienta que lo sustituya.

f. Responsable de la calificación de Reserva de la información pública por razones de defensa y seguridad nacional, seguridad pública o relaciones internacionales. La calificación de reservada de la información prevista en la Ley, corresponderá exclusivamente al jefe de la dependencia o área responsable de la generación, posesión, control o custodia de la información, o funcionario o empleado del nivel

directivo que, por su completo e integral conocimiento de la información pública, pueda garantizar que la calificación sea razonable y proporcionada.

g. Temporalidad de la reserva. Sin perjuicio de lo señalado en la Ley y del período máximo de reserva de la información, la información respectiva debe divulgarse si desaparecen las condiciones que justificaban su reserva.

El término máximo de quince (15) años a que se refiere el artículo 22 de la Ley 1712 de 2014 empezará a contarse a partir de la fecha en que la información se genera.

h. Seguridad y Accesibilidad y Otras Directrices.

1) Formato alternativo: Para efectos de lo previsto en el artículo 8° de la Ley 1712 de 2014, se entenderá por formato alternativo, la forma, tamaño o modo en la que se presenta la información pública o se permite su visualización o consulta para los grupos étnicos y culturales del país, y para las personas en situación de discapacidad, en aplicación del criterio diferencial de accesibilidad.
2) Accesibilidad en medios electrónicos para población en situación de discapacidad: Todos los medios de comunicación electrónica dispuestos para divulgar la información deberán cumplir con las directrices de accesibilidad que dicte el Ministerio de Tecnologías de la Información y las Comunicaciones a través de los lineamientos que se determinen en la Estrategia de Gobierno en línea.
3) Accesibilidad a espacios físicos para población en situación de discapacidad: Los sujetos obligados deben cumplir con los criterios y requisitos generales de accesibilidad y señalización de todos los espacios físicos destinados para la atención de solicitudes de información pública y/o divulgación de la misma, conforme a los lineamientos de la Norma Técnica Colombiana 6047, "Accesibilidad al medio físico. Espacios de servicio al ciudadano en la Administración Pública. Requisitos", o la que la modifique o sustituya, atendiendo al principio de ajustes razonables establecido en dicha norma.
4) Publicación del mecanismo o procedimiento para participar en la formulación de políticas o en el ejercicio de las facultades del sujeto obligado. Los sujetos obligados, de acuerdo con el régimen legal aplicable, deben publicar los procedimientos a que deben sujetarse los ciudadanos, usuarios o interesados en participar en la formulación de políticas y en el control o evaluación de la gestión institucional, indicando: los sujetos que pueden participar, los medios presenciales y electrónicos, y las áreas responsables de la orientación y vigilancia para su cumplimiento.
5) Publicación del programa de gestión documental. El Programa de Gestión Documental (PGD) debe ser publicado en la página web de la respectiva entidad, dentro de los siguientes treinta (30) días posteriores a su aprobación por parte del Comité de Desarrollo Administrativo de la Entidad en las entidades del orden nacional o el Comité Interno de Archivos en las entidades del orden territorial, siguiendo los lineamientos del Manual de Gobierno en Línea., Así mismo sus programas de gestión documental deberán tener en cuenta la protección de la información y los datos personales de conformidad con la Ley 1273 de 2009 y la Ley 1581 de 2012.
6) El Archivo General de la Nación en conjunto con el Ministerio de Tecnologías de la Información y las Comunicaciones, y la delegada de la protección de datos de la Superintendencia de Industria y Comercio deberán dar las directrices y las políticas para proteger la información y los datos personales que reposan en bases de datos y documentos electrónicos en los programas de gestión documental.

7) Plan de Capacitación. deberán incluir en sus planes anuales de capacitación los recursos necesarios para capacitar en el alcance y desarrollo del PGD, a los funcionarios de los diferentes niveles de la entidad.

Armonización con otros sistemas administrativos y de gestión. El Programa de Gestión Documental (PGD) debe armonizarse con los otros sistemas administrativos y de gestión establecidos por el gobierno nacional o los que se establezcan en el futuro.