SOCIEDAD TEQUENDAMA

MSPI
MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Bogotá, D.C.

ELABORO	REVISO	APROBÓ
Gloria Peña	Christian González	Christian González
Jefe de Tecnología de la Información y las Comunicaciones	Secretaria General	Secretaria General
Firma:	Firma:	Firma:

Contenido

1. INTRODUCCIÓN

El ministerio de Tecnología de la Información y las Comunicaciones (MINTIC) a través de la Dirección de Gobierno Digital, dando cumplimiento a sus funciones: pública 'El modelo de Seguridad y Privacidad de la Información (MSPI)', el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI. El modelo Integrado de Planeación y Gestión (MIPG) y la Guía para la Administración del Riesgo y el Diseño de Controles en entidades públicas (Documento emitido por el Departamento Administrativo de la Función Pública. Última actualización diciembre de 2020).

El Modelo de Seguridad y Privacidad es un modelo dinámico que se actualizara con las mejores prácticas de seguridad teniendo en cuenta la norma 27001, legislación de la Ley de Protección de datos personales, Transparencia y acceso a la información pública, Gobierno digital y Seguridad digital, las cuales se deben tener en cuenta para la gestión de la información.

2. OBJETIVOS

El Plan de Seguridad de la Información es un documento que tiene por objetivo trazar y planificar la manera como la Sociedad Tequendama (ST) continuará con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI)

3. ALCANCE

Se definirán las actividades a cumplir teniendo como marco de referencia los lineamientos de Gobierno y Seguridad digital. Para esta labor se involucran todos los procesos de la Sociedad Tequendama (ST), los cuales deberán entregar la información que se requiera al grupo encargado de adelantar la implementación.

4. LIMITES

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas.

Procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos

5. REFERENCIA NORMATIVA

Ley 1581 de 2012. Disposiciones Generales para tratamiento de datos personales
Ley 1273 de 2009. Congreso de la República. Por medio del cual se modifica el código penal, se crea un bien jurídico tutelado-Denominado "De la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones

Ley 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
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.
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
Directiva permanente Ministerio de Defensa N° 018 de 2014. Políticas de seguridad de la información para el Sector Defensa
Que la Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones", tiene como objeto regular el derecho de acceso a la Información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.
Que el artículo 147 de la Ley 1955 de 2019 "Por el cual se expide el Plan Nacional de Desarrollo 2018-2022." Pacto por Colombia, Pacto por la Equidad" en relación con la Transformación Digital Pública establece que: "Las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para este propósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones (...)". Asimismo, especifica que Los proyectos estratégicos de transformación digital se orientarán, entre otros, por el principio de "Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales."
Acorde con este principio, que el artículo 148 de la Ley 1955 de 2019 señala que "Todas las entidades de la administración pública deberán adelantar las acciones que señale el Gobierno nacional a través de Ministerio de Tecnologías de la Información y las Comunicaciones para la implementación de la Política de Gobierno Digital", y dentro de las acciones prioritarias se encuentra el cumplimiento de los lineamientos y estándares para el incremento de la confianza y la seguridad digital.
Que el artículo 2.2.35.3 del Decreto 415 de 2016 "Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para e/ fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones"' establece dentro de los objetivos del fortalecimiento institucional, numeral 3 "Desarrollar los lineamientos en materia tecnológica, necesarios para definir políticas, estrategias y prácticas que habiliten la gestión de la entidad y/o sector en beneficio de la prestación efectiva de sus servicios y que a su vez faciliten la gobernabilidad y gestión de las Tecnologías de la Información y las Comunicaciones (TIC). Así mismo, velar por e/ cumplimiento y actualización de las políticas y estándares en este material'.
Que el parágrafo del artículo 16 del 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" señala que las autoridadesdeberán disponer de una estrategia de seguridad digital siguiendo los lineamientosque emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
Que mediante el Decreto 338 del 8 de marzo de 2022 "Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías

de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la Seguridad Digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones" establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital.
Que mediante la Resolución 463 del 9 de febrero de 2022 del Ministerio de Defensa Nacional, "Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones.", indica en relación con la seguridad en las soluciones con tecnologías de la nube, que el Sector Defensa tendrá la responsabilidad de asegurar que la adopción, implementación o migración de una solución basada en Tecnologías en la Nube sea confiable y segura, teniendo en cuenta la disponibilidad para proporcionar, de manera prospectiva, los servicios de tecnologías de la información. Así mismo, se deberá establecer las necesidades particulares de seguridad de cada solución, las pruebas específicas y la periodicidad.
Que a través de la Directiva Permanente 0018 del 19 de junio de 2014 del Ministerio de Defensa Nacional, se establecen y difunden los criterios con el propósito de preservar la confidencialidad, integridad y disponibilidad de la información a fin de fortalecer la continuidad de las actividades administrativas, operativas y logísticas del sector defensa.
Que mediante la Directiva Permanente 03 del 23 de enero de 2019 "Lineamientos para la definición de la Política de Tratamiento de Datos Personales en el Ministerio de Defensa Nacional", se establecieron los lineamientos para la adopción de la política frente a la recolección, manejo tratamiento y protección de datos personales y privacidad de todas las personas con el propósito de garantizar y proteger el derecho fundamental de habeas data. Así mismo, unificar los criterios a publicar en sus respectivos sitios web relacionados con los términos y condiciones de uso.
Que mediante Directiva Presidencial 03 del 15 de marzo de 2021 "Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos", frente a la Seguridad Digital, precisa directrices con el fin de fortalecer las capacidades y la funcionalidad de las entidades en términos de ciberseguridad y resiliencia corporativa.
Que mediante Directiva Presidencial 02 del 24 de febrero de 2022 "Reiteración de la política pública en materia de seguridad digital." se reitera que en desarrollo de la Política de Gobierno Digital y su Manual de Implementación, es responsabilidad de los representantes legales de las entidades públicas del orden nacional, coordinar, hacer seguimiento y verificación de la implementación de la Política de Gobierno Digital, así como garantizar el desarrollo integral de la política al interior de sus entidades, entendiendo que esta es un eje transversal y apalancador de su gestión interna, que apoya el desarrollo de las políticas de gestión y desempeño institucional.
Que, se hace necesario adoptar la Directiva Permanente 0018 del 19 de junio de 2014 del Ministerio de Defensa Nacional -DIR2014-18- "Políticas de Seguridad de la Información para el Sector Defensa" así como la Resolución 7870 del 26 de diciembre de 2022, por la cual el Ministerio de Defensa Nacional procedió a emitir y adoptar la Política General de Seguridad y Privacidad de la información, seguridad Digital, Ciberseguridad y Continuidad de los servicios tecnológicos en las Unidades Ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y entidad adscritas y vinculadas al Sector Defensa, y se dictan otras disposiciones.", con el fin de dar aplicación a las normas, políticas y directivas que sobre el particular ha expedido el Ministerio de Defensa.
Que de acuerdo con el artículo 2 de la Resolución7870 del 26 de diciembre de 2022, el Ministerio de Defensa Nacional, protege, preserva y administra la confidencialidad, integridad, disponibilidad y autenticidad de la información, así como la seguridad digital, ciberseguridad y

gestión de la continuidad de la operación, conforme a los procesos de cada una de las entidades, dando cumplimiento a los requisitos legales y reglamentarios; previniendo igualmente los incidentes mediante la gestión de riesgos integrales en seguridad y privacidad de la información, seguridad digital, ciberseguridad y la implementación de controles de seguridad físicos y digitales, orientados a la mejora continua en la gestión y el alto desempeño del Sistema de Gestión de Seguridad de la Información.
Documento CONPES 3854 de abril 11 de 2016, Política Nacional de Seguridad Digital
Documento CONPES 3995 de Julio 1 de 2020 Política Nacional de confianza y seguridad Digital

6. DEFINICIONES

- **Acceso a la Información Pública.** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
- **Activo.** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo de Información.** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Archivo.** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
- **Amenazas.** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo.** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Auditoría.** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- **Autorización.** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- **Bases de Datos Personales.** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Ciberseguridad.** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio.** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software),

redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **Control.** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos.** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)
- **Datos Personales.** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos.** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
- **Datos Personales Privados.**Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Mixtos.** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles.** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
- **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).
- **Derecho a la Intimidad.** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- **Encargado del Tratamiento de Datos.** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- **Gestión de incidentes de seguridad de la** información**.** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada.** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Información Pública Reservada.** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Ley de Habeas Data.** Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública.** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales.** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Plan de continuidad del negocio.** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos.** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Privacidad.** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Registro Nacional de Bases de Datos. Directorio público de las bases de datos** sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- **Responsabilidad Demostrada.** Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- **Responsable del Tratamiento de Datos.** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).
- **Riesgo.** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información.** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGS.** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Titulares de la información.** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- **Tratamiento de Datos Personales.** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad.** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Vulnerabilidad.** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000). .
- **Partes interesadas (Stakeholder).** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

7. DESCRIPCIÓN GENERAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. (MSPI)

La Sociedad Tequendama planea la implementación del modelo conforme a las siguientes fases.

- Fase de Diagnostico. identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información,
- Fase de Planificación. elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo
- Fase de implementación. implementación de la planificación realizada en la fase anterior del MSPI

- Fase de Evaluación y desempeño. proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas
- Fase de Mejora continua. consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.
- Modelo de madurez. Este esquema permite identificar el nivel de madurez del MSPI en el que se encuentran las entidades, midiendo la brecha entre el nivel actual de la entidad y el nivel optimizado.

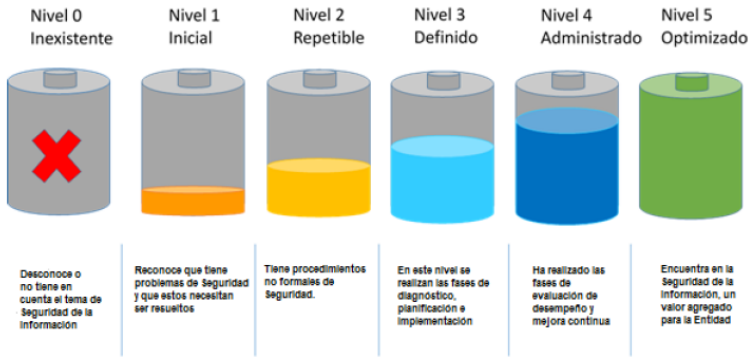

Figura 7. Niveles de madurez

Tabla 6 – Características de los Niveles de Madurez Nivel
Inexistente
● Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo no están alineados a un Modelo de Seguridad.
● No se reconoce la información como un activo importante para su misión y objetivos estratégicos.
● No se tiene conciencia de la importancia de la seguridad de la información en la entidad.
Inicial
● Se han identificado las debilidades en la seguridad de la información.
● Los incidentes de seguridad de la información se tratan de forma reactiva.
● Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.
Repetible
● Se identifican en forma general los activos de información.
● Se clasifican los activos de información.
● Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información.
● Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión.
● La entidad cuenta con un plan de diagnóstico para IPv6.
Definido
● La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información.
● La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información.
● La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas.
● La Entidad tiene procedimientos formales de seguridad de la Información

● La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información.
● La Entidad ha realizado un inventario de activos de información aplicando una metodología.
● La Entidad trata riesgos de seguridad de la información a través de una metodología.
● Se implementa el plan de tratamiento de riesgos.
● La entidad cuenta con un plan de transición de IPv4 a IPv6.
Administrado
● Se revisa y monitorea periódicamente los activos de información de la Entidad.
● Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información.
● Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro.
● La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.
Optimizado
● En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización.
● Se utilizan indicadores de efectividad para establecer si la entidad

8. ADOPCION RESOLUCION 7870 26/diciembre/2022

Documento elaborado por el área jurídica.

ARTÍCULO PRIMERO. Adóptese la Resolución 7870 del 26 de diciembre de 2022, por la cual el Ministerio de Defensa Nacional procedió a emitir y adoptar la **Política General de Seguridad y Privacidad de la información, Seguridad Digital, Ciberseguridad y Continuidad** de los servicios tecnológicos en las Unidades Ejecutoras o dependencias del Ministerio de Defensa Nacional, la Policía Nacional y entidad adscritas y vinculadas al Sector Defensa, y se dictan otras disposiciones.", con el fin de dar aplicación a las normas, políticas y directivas que sobre el particular ha expedido el Ministerio de Defensa; y la Directiva Permanente 0018 del 19 de junio de 2014 del Ministerio de Defensa Nacional -DIR2014-18- "Políticas de Seguridad de la Información para el Sector Defensa".

ARTÍCULO SEGUNDO. Delegar en la Secretaría General, de conformidad con el parágrafo del artículo sexto de la Resolución 7870 del 26 de diciembre de 2022, en relación con la impleentación de esta resolución, las siguientes funciones:

· Verificar el cumplimiento de la resolución mencionada y demás normas que la desarrollen, adicionen o modifiquen.

· Promover la adopción de medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital.

· Promover el desarrollo de una cultura de seguridad de la información y ciberseguridad a través de campañas de sensibilización y concientización.

· Adoptar la seguridad digital y ciberseguridad con un enfoque preventivo y proactivo, priorizando la protección de datos personales e información sensible de la entidad o que goza de reserva legal, al igual que los servicios y sistemas de información e infraestructura críticas.

· Fungir como único canal de comunicación autorizado para hacer pronunciamientos oficiales ante entidades externas, medios de comunicación o la ciudadanía, reportará los

incidentes que afecten la infraestructura crítica y la Seguridad Nacional ante las autoridades competentes.

· Designar al Responsable de Seguridad de la Información representante de la Alta Dirección para el Modelo de Seguridad y Privacidad de la Información (MSPI), con el fin de apoyar las actividades y controles necesarios para llevar a cabo la implementación y la mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI) en su entidad.

· Gestionar los recursos financieros requeridos para la implementación del (MSPI).

· Ordenar la inclusión, de temas relacionados con seguridad de la información y ciberseguridad, en las materias y cursos de tecnología que se dictan en las escuelas de formación y capacitación de las Fuerzas Militares y Policía Nacional.

· Apoyar la creación de los respectivos Equipos de Respuesta a Emergencia Informáticas (CSIRT) y Centros de Operaciones de Seguridad (SOC), con el propósito de apoyar a la gestión de incidentes.

ARTÍCULO TERCERO. Delegar en la Oficina de Tecnologías e Información y las Comunicaciones, el cumplimiento de la Resolución 7870 del 26 de diciembre de 2022, para lo cual deberá realizar las siguientes actividades:

Dar cumplimiento a lo establecido en el artículo 18, en relación con la adopción de las medidas necesarias para asegurar la transferencia y seguridad de la información, incluyendo la contenida en los mensajes electrónicos. Para lo cual deberá tener en cuenta los lineamientos establecidos en el artículo mencionado.

Dar cumplimiento al artículo 19 en relación con la Política General de la estrategia de seguridad digital, para lo cual deberá liderar la implementación del Modelo de Seguridad y privacidad de la Información (MSPI), articularlo debidamente con el habilitador de seguridad y privacidad de la política de Gobierno Digital, de acuerdo con los lineamientos emitidos en la Resolución 500 del 10 de marzo de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones. Dicha estrategia deberá dar aplicación a los lineamientos y criterios establecidos en el mismo artículo 19. Igualmente, en relación con la Política para la gestión de riesgos de la seguridad de la información, seguridad digital y ciberseguridad,

dar cumplimiento al artículo 20. Deberá implementar los planes y controles para mitigar los riesgos que puedan afectar la seguridad digital y física de acuerdo con el resultado de análisis y evaluación de riesgos, y cumplir con las demás características y responsabilidades establecidas en el artículo 20 de la misma resolución.

En relación con la Política de tratamiento para la gestión de incidentes de Seguridad digital, deberá dar cumplimiento a lo establecido en el artículo 21 para lo cual deberá gestionar los incidentes de seguridad digital y ciberseguridad y deberá coordinar las tareas de seguridad informática, para lo cual deberá cumplir con los lineamientos y criterios establecidos en ese artículo.

En el marco de lo señalado deberá liderar el relacionamiento en la materia con los Equipos de Respuesta a Emergencias Informáticas (CSIRT) del Ministerio de Defensa, con el fin de coordinar con ellos las capacidades de ciberseguridad y ciberdefensa.

Dar cumplimiento y ejecución a lo establecido en el parágrafo del artículo 22, como la encargada de elaborar el análisis del impacto del negocio (BIA) y el plan tecnológico de la entidad.

En relación con la política de continuidad de la operación, dar cumplimiento al mismo artículo 22, por lo cual será la encargada de la operación y administración de los recursos tecnológicos que soportan la operación, definir e implementar el plan de continuidad tecnológico del negocio, así como los procedimientos de continuidad y de contingencia para cada una de las plataformas tecnológicas críticas bajo su responsabilidad y cualquier estrategia orientada a generar el diagnóstico inicial, la contención, la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de riesgos de seguridad de la información, seguridad digital y ciberseguridad, para lo cual deberá dar aplicación a los criterios establecidos en ese artículo.

ARTÍCULO CUARTO. De conformidad con lo establecido en el parágrafo del artículo 22 de la Resolución 7870 del 26 de diciembre de 2022, delegar en laOficina de Planeación o quien haga sus veces, como la oficina encargada de liderar el Plan de Continuidad del Negocio de esta sociedad.

ARTÍCULO QUINTO. De conformidad con lo señalado en el artículo 23 de la Resolución 7870 del 26 de diciembre de 2022, todos los servidores públicos, contratistas o terceros que hagan uso de los recursos tecnológicos de la Sociedad Tequendama tienen la responsabilidad de cumplir cabalmente las políticas establecidas para su uso aceptable, entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación y, por ende, el cumplimento de la misión institucional. Deberán cumplir con las siguientes directrices:

· Los bienes de cómputo no pueden ser utilizados con fines personales, estos se emplearán de manera exclusiva y bajo la completa responsabilidad del servidor público o contratista al cual han sido asignados, únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas.

· La Oficina de Tecnología e Información deberá establecer y aplicar controles respecto al uso adecuado de los activos de información, así como la verificación de cumplimiento del software base y de aplicaciones, para prevenir la descarga, instalación y uso de software no licenciado y/o no autorizado, definiendo, manteniendo y controlando la lista de software y aplicaciones autorizadas para ser instaladas en las estaciones de trabajo de los usuarios, cumpliendo los criterios de autenticidad, vigencia, términos y condiciones legales para la utilización de la licencia.

· En caso de que el servidor público, contratista y/o terceros deba hacer uso de equipos ajenos a la Sociedad Tequendama, éstos deberán cumplir con la legalidad del Software instalado, antivirus licenciado, actualizado y solo podrá conectarse a la red institucional, si es autorizado por la oficina de Tecnologías o quien haga sus veces.

· Es responsabilidad de los servidores públicos, contratistas y terceros mantener copias de seguridad de la información contenida en sus estaciones de trabajo y entregarlas al finalizar la vinculación con la Entidad para su custodia.

· Está expresamente prohibido el almacenamiento en los discos duros de computadores de escritorio, portátiles o discos virtuales de red, de archivos de video, música y fotos que

no sean de carácter institucional o que atenten contra los derechos de autor o propiedad intelectual de los mismos. · No está permitido ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos o información física que pueda estar expuesta a daño parcial o total y, por ende, a la pérdida de la integridad de ésta.

· No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro eléctrico a los equipos de cómputo, salvo en aquellos casos autorizados expresamente por la dependencia responsable.

· Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, son las designadas para tal labor por la Oficina de Tecnología e Información.

· La Oficina de Tecnología e Información realizará monitoreo sobRe los dispositivos de almacenamiento externos como USB, CD-ROM, DVD, Discos Duros externos, entre otros, con el fin de prevenir o detectar fuga de información.

· La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es la que tenga bajo su responsabilidad dicha función previa coordinación con la Oficina de Tecnología e Información, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de la gestión de bienes de la respectiva entidad Sector Defensa.

· La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes deberá ser informada de inmediato a la Oficina de Tecnología e Información por el servidor público, contratista o tercero a quien se le hubiere asignado; así mismo, deberá reponerse a la entidad o aplicar los procedimientos establecidos para este tipo de siniestros que estime la entidad.

· La pérdida de información deberá ser informada con detalle a la Oficina de Tecnología e Información, a través de la Mesa de Servicios o de ayuda, como incidente de seguridad.

· Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información física o digital deberá ser reportado a la mayor brevedad a la Oficina de Tecnología, a través de la mesa de Servicios, siguiendo el procedimiento establecido.

· La Oficina de Tecnología es la dependencia autorizada para la administración del software o para autorizar su administración a otra dependencia, la cual no deberá ser copiado, suministrado a terceros ni utilizado para fines personales.

· Todo acceso a la red institucional deberá ser informado, autorizado y controlado por la Oficina de Tecnología.

· La conexión a la red Wifi institucional para servidores públicos y contratistas deberá ser administrada desde la Oficina de Tecnología, mediante un SSID (Service Set Identifier) único; la autenticación deberá ser con usuario y contraseña de directorio activo u otro tipo de autenticación cuando aplique para la Entidad.

· La conexión a la red Wifi institucional para visitantes deberá tener un SSID y las contraseñas serán administradas por la Oficina de Tecnología y las contraseñas deberán cambiar los lunes de cada semana, solo estarán disponibles en el horario laboral definido

y la conexión solo será para el servicio de internet y estará restringida para la conexión a servicios institucionales.

· La red Wifi para servidores públicos y contratistas estará disponible para sus equipos personales, teniendo en cuenta las capacidades técnicas, contractuales y lineamientos de seguridad establecidos por el Ministerio.

· Las redes inalámbricas (Wifi) de servicio en las entidades, deben ser redes para acceso y consulta de internet y no para que por medio de estas se administren infraestructuras internas o se acceda a servicios misionales internos desde dispositivos no corporativos, se exceptúan los casos autorizados por la Oficina de Tecnología a funcionarios que cuenten con el perfil de administradores y se encuentre realizando actividades de trabajo remoto.

· Los equipos deben quedar apagados cada vez que el servidor público, contratista o tercero no se encuentre en la oficina o durante la noche; esto, con el fin de proteger la seguridad y distribuir bien los recursos de las entidades Sector Defensa; se exceptúa aquellos casos en que se esté realizando trabajo remoto.

· Cuando se utilicen aplicaciones de mensajería instantánea para actividades institucionales, deberán adoptarse políticas de seguridad y términos de uso de las aplicaciones, evaluando previamente los riesgos de vulnerabilidades de afectación a la confidencialidad, integridad y disponibilidad de la información.

· Los servicios de Tecnologías en la Nube deben aplicar las medidas de seguridad necesarias para garantizar la integridad, disponibilidad y confidencialidad de la información de la institución, así como cumplir con los requisitos establecidos en la normatividad vigente y con los niveles de seguridad adecuados para los servicios que presta cada entidad del Sector Defensa.

· Todos los recursos informáticos y la infraestructura de procesamiento, comunicaciones y seguridad informática incluyendo los servicios en la nube de la Sociedad Tequendama, deberán estar protegidos mediante herramientas y software de seguridad que prevenga el ingreso de código malicioso a la red interna, así como mecanismos para detectar, prevenir y recuperar posibles fallos.

· La Oficina de Tecnologías será responsable de que sus usuarios se mantengan actualizados acerca de los riesgos de infección de código malicioso provenientes de correos electrónicos, páginas Web, el intercambio de archivos o cualquier otra actividad de su operación diaria que pueda ser aprovechada por una amenaza.

· Todo dispositivo móvil personal que requiera acceder a los servicios tecnológicos de la entidad y que transmita y/o almacene información sensible debe ser monitoreado a través de la herramienta tecnológica definida por la Oficina de Tecnología o quien haga sus veces.

Sobre el uso de dispositivos Institucionales de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros. la Oficina de Tecnología propenderá por el correcto uso, manejo y control de riesgos de seguridad de los dispositivos institucionales de computación móvil como herramienta de trabajo asignada a los servidores públicos, contratistas o terceros, para facilitar las comunicaciones, cuando así se estime pertinente; para lo cual deberá:

Verificar que los dispositivos móviles cuenten con los siguientes controles:

Sistema de autenticación, como un patrón, código de desbloqueo o una clave para el acceso al mismo, uso de software de antivirus suministrado por la Entidad, restricción de privilegios administrativos para los usuarios y uso de Software licenciado suministrado por la Entidad.

· Asegurar la conexión de los dispositivos móviles a la infraestructura tecnológica institucional, estableciendo los mecanismos de control necesarios para proteger la infraestructura tecnológica institucional.

· Implementar técnicas criptográficas para cifrar la información crítica almacenada en los dispositivos de computación móvil.

· Mantener actualizados los sistemas operativos, navegadores, manejador de contenidos, librerías y, en general, todo el software, con las respectivas actualizaciones de seguridad liberadas por los fabricantes.

Los servidores públicos que pertenezcan a las entidades del Sector Defensa deben cumplir con las siguientes responsabilidades frente al correcto uso de los dispositivos Institucionales de computación móvil:

· Los teléfonos móviles y/o teléfonos inteligentes institucionales, debe permanecer encendidos y cargados como mínimo durante las horas laborales.

· El uso del dispositivo móvil suministrado debe ser para realizar actividades propias de su cargo o funciones asignadas en la entidad.

· No están autorizados a cambiar la configuración, ni a la desinstalación de software de los equipos móviles institucionales posterior a su recibo; únicamente se deben aceptar y aplicar las actualizaciones.

· Evitar hacer uso de los dispositivos móviles en lugares con algún riesgo de seguridad, con el fin de evitar el extravío o hurto del equipo.

· No se debe hacer uso de los dispositivos móviles en redes inalámbricas públicas.

Sobre el uso del correo electrónico institucional.

· El único servicio de correo electrónico autorizado para el manejo o transmisión de la información institucional en la Entidad es el asignado por la Oficina de Tecnología, con el dominio de la entidad, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando cualquier tipo de ataque cibernético. Así mismo deberán contener una sentencia de confidencialidad, que será diseñada por la oficina de Tecnología e Información, con el apoyo de la Oficina de Comunicaciones y la oficina Jurídica, o similares en la entidad.

· El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional y debe contener cuando aplique la firma digital de la entidad por medio de un método criptográfico; en consecuencia, no puede ser utilizado con fines personales, económicos, comerciales o cualquier otro fin ajeno a los propósitos de la Entidad.

· En cumplimiento de la iniciativa institucional del uso aceptable del papel y la eficiencia administrativa, se debe preferir el uso del correo electrónico al envío de documentos físicos, siempre que la Ley lo permita.

· La Oficina de Tecnología implementará herramientas tecnológicas que prevengan la pérdida o fuga de información de carácter reservado o clasificado, de conformidad con las leyes estatutarias 1266 de 2008, 1581 de 2012, 1621 de 2013 y 1712 de 2014.

· Se permite el envío masivo de correos de carácter institucional desde cuentas corporativas, los cuales deben cumplir con las características de comunicación e imagen corporativa y ser asignadas a un responsable para garantizar el correcto uso de estas.

· Para facilitar la gestión de correo electrónico de directivos, el titular debe solicitar a la respectiva mesa de servicios la delegación del buzón correspondiente, relacionando os colaboradores que podrán escribir o responder en nombre del titular, con el fin de mitigar la suplantación.

· Todo mensaje SPAM, cadena, de remitente o contenido sospechoso, debe ser inmediatamente reportado a la Oficina de Tecnología a través de la respectiva Mesa de Servicios o similar, como incidente de seguridad según el procedimiento establecido, y deberán acatarse las indicaciones recibidas para su tratamiento.

· La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, o cualquier otra ajena a los fines de la entidad.

· Está expresamente prohibido el uso del correo institucional para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y que atenten contra la integridad moral y/o buena imagen de las personas o instituciones.

· Está expresamente prohibido distribuir información catalogada como clasificada o reservada de las entidades del Sector Defensa a otras entidades o ciudadanos sin la debida autorización del despacho del Ministro, Viceministros, Secretario General, Secretario de Gabinete, Comandante General de las Fuerzas Militares, Jefe de Estado Mayor Conjunto de las Fuerzas Militares, Comandantes y Segundos Comandantes de Fuerza, Director General y Subdirector General de la Policía Nacional, representante legal de las entidades adscritas o vinculadas, Oficinas de Comunicaciones, Oficinas de Planeación, Oficinas de Estudios Sectoriales o las que hagan sus veces, en los casos que aplique.

· El cifrado de los mensajes será necesario siempre que la información transmitida desde un correo electrónico institucional esté catalogada como clasificada o reservada en el inventario de activos de información o en el marco de la Ley Colombiana vigente.

· Está expresamente prohibido distribuir, copiar, reenviar información propiedad de la entidad a través de correos personales o sitios web diferentes a los autorizados en el marco de sus funciones u obligaciones contractuales.

· La Oficina de Tecnología debe coordinar internamente la identificación de los buzones de correo institucionales que se considere su contenido como información relevante para la Entidad y por ello se hace necesario salvaguardar la información de acuerdo con las regulaciones vigentes en cuanto a preservación y conservación documental establecidas

por el Archivo General de la Nación y Ministerio de Tecnologías de la Información y Comunicaciones.

La Sociedad Tequendama se reservan el derecho de monitorear los accesos y el uso de los buzones de correo institucional de todos sus servidores públicos o contratistas. Además, podrá realizar copias de seguridad del correo electrónico institucional en cualquier momento sin previo aviso y limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información propios o de terceros operados en la Sociedad Tequendama, previa solicitud expresa del Ministro de Defensa, Viceministros, Comandante General de las Fuerzas militares, Comandante de Fuerza, Director de la Policía Nacional, del nominador, ordenador del gasto, supervisor del contrato, jefe inmediato, Control Disciplinario Interno, Gestión del Talento Humano, y de la Oficina de Tecnología.

Sobre el uso de Internet: La Oficina de Tecnología, a través del Jefe de Seguridad de la Información, establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones y será responsabilidad de los colaboradores las siguientes, entre otras:

Los servicios a los que un determinado usuario pueda acceder en internet dependerán del rol o funciones que desempeña en las entidades del Sector Defensa y para las cuales esté formal y expresamente autorizado por su jefe o supervisor, y solo se utilizará para fines laborales.

No está permitido enviar, descargar y visualizar páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor o que atenten contra la integridad moral de las personas o de las instituciones.

No está permitido acceder a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas por la política de navegación de la Sociedad Tequendama o el Ministerio de Defensa.

•No está permitido enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida.

•No está permitido propagar intencionalmente virus o cualquier tipo de código malicioso.

•La Sociedad Tequendama de acuerdo con su tamaño, despliegue de infraestructura tecnológica, superficie de exposición e internet y los servicios y sistemas esenciales que gestionen, debe conformar un Grupo de Seguridad Digital y nombrar el oficial de seguridad de la información, quien será el encargado de verificar la correcta aplicación de las políticas y estrategias vigentes en su entidad dentro del marco del cumplimiento de las misión y funciones asignadas.

•La Oficina de Tecnología debe implementar protocolos y políticas de acceso remoto que impidan a los usuarios escalar privilegios y que mitigue el riesgo de acceso no autorizado a recursos o información.

•La Oficina de Tecnología se reserva el derecho de monitorear los accesos y el uso del servicio de Internet, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro uso ajeno a los fines institucionales.

Del uso de las redes sociales: Todos los sentidores públicos son responsables de la información que generan, acceden y procesan, así como de evitar su uso indebido, para lo cual se dictan los siguientes lineamientos:

•Las redes sociales de carácter institucional no deben ser abiertas a nombre propio de funcionarios o contratistas sino de la entidad.

•El funcionario responsable del manejo de las redes sociales institucionales debe garantizar el uso adecuado de las mismas.

•El uso de las redes sociales de carácter institucional debe ser controlada por la Oficina de comunicación de la entidad, con el fin de contar con niveles de protección adecuados para un uso correcto y seguro de estas plataformas en apoyo con la Oficina de Tecnología.

•Se deben utilizar soluciones de seguridad, configurar correctamente los usuarios en las redes sociales, utilizar cuando sea posible un segundo factor de autenticación y el protocolo HTTPS para la navegación, entre otros.

•Se requiere no utilizar un usuario con permisos de administrador al momento de navegar en las redes sociales, y que cada funcionario permitido cuente con sus propios perfiles. Esta es una forma de minimizar el impacto en caso de que ocurra un incidente.

•No utilizar la contraseña de una red social en otros sitios de internet y nunca compartirla, aplicar reglas de contraseña segura, evitar utilizar computadoras públicas para ingresar en las redes sociales institucionales.

Sobre el uso del escritorio, pantalla limpias y periféricos: Todos los servidores públicos, contratistas o terceros que laboran en la Sociedad Tequendama y que hagan uso de estaciones de trabajo, deberán acatar las siguientes disposiciones:

•En horas no hábiles, o cuando los sitios de trabajo se encuentren desatendidos, dejar los medios que contengan información crítica protegida bajo llave.

•Bloquear su estación cada vez que se retiren de su puesto de trabajo y solo se podrá desbloquear con la contraseña del mismo usuario que lo bloqueó.

•Tomar las medidas de seguridad necesarias en el uso de sus contraseñas, para evitar que estas sean conocidas por personal interno o externo a la Entidad.

•Cuando se imprima o digitalice documentos con información pública clasificada o pública reservada, éstos deben retirarse inmediatamente de dichos dispositivos.

•Los dispositivos de impresión y digitalización deben permanecer limpios de documentos.

•Los documentos que contengan información institucional sensible no deben ser reutilizados y destruirse de acuerdo con los parámetros y normatividad vigente establecida en la ley de Archivo General vigente.

Sobre el uso de los sistemas o herramientas de Información: Todos los servidores públicos, contratistas o terceros que laboran en la Sociedad Tequendama son responsables de la protección de la información que acceden y procesan, así como de evitar su pérdida, alteración, destrucción y uso indebido, para lo cual se dictan los siguientes lineamientos:

•Las credenciales de acceso a la red y a los recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible.

•Es responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos asignados de acuerdo con las políticas de administración de usuarios establecidas en la entidad.

•Es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.

•Cuando se ausenta por vacaciones, permiso, comisiones, excusas médicas, entre otros, deberá solicitar a través de la mesa de servicios o similar, el bloqueo de acceso a la estación de trabajo y la cuenta de correo electrónico institucional, a la Oficina de Tecnología o quien haga sus veces , así mismo si tiene asignado accesos a sistemas de información, deberá reportar a los entes correspondientes para que inactiven las respectivas licencias, con el fin de evitar la fuga de la información, el acceso a terceros, lo cual pueda generar daño, alteración o uso indebido a la información, así como la suplantación de identidad. La dependencia de Gestión del Talento Humano, y supervisores de los contratos, deberán reportar inmediatamente cualquier tipo de novedad que presenten los servidores públicos, contratistas o terceros a la Oficina de Tecnología.

•Cuando cesa sus funciones o culmina la ejecución de contrato con la respectiva entidad del Sector Defensa, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente; la información del servidor público o contratista será almacenada en los repositorios establecidos por cada una de las Entidades del Sector Defensa de acuerdo a sus políticas de archivo y conservación de la información.

•Cuando cesa sus funciones o culmina la ejecución de contrato con la respectiva entidad, el jefe inmediato o supervisor es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual, de acuerdo con la normativa vigente.

•Dar estricto cumplimiento a la reglamentación vigente sobre derechos de autor.

ARTÍCULO SEXTO. Medición. La medición estará en cabeza y liderazgo de la Oficina de Tecnologías e Información, y la aplicación de indicadores de gestión al modelo de operación del marco de seguridad y privacidad de la información de la Sociedad Tequendama S.A., y están orientados principalmente en la medición de efectividad, eficacia y eficiencia de los componentes de implementación y gestión de los planes de seguridad digital, definidos en esta sociedad. En este sentido, en cumplimiento del artículo 24 de la Resolución 7870 de 2022, se dará aplicación a la "Guía No 9 de indicadores de gestión de seguridad de la información' emitida por el MinTIC y el "esquema 9. Consolidación de los Planes y Tratamiento de Riesgo", de la "Guía para a la administración de/ Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles Entidades Públicas (Ver 5 — 20201' emitidas por el DAFP.

ARTÍCULO SÉPTIMO. Cumplimiento. La Gerencia General verificará el cumplimiento de la presente Resolución con el apoyo y acompañamiento de la Secretaría general y la Oficina de Tecnologías e Información de esta sociedad, en particular la definición de una estrategia propuesta por ésta última oficina para aprobación del Comité directivo de la sociedad, que permita brindar servicios, controles y condiciones que garanticen la

Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de las entidades.

ARTÍCULO OCTAVO. La oficina de Control Interno, durante la realización de las auditorías, validará y consignará en sus informes el nivel de cumplimiento de los lineamientos de la Resolución 7870 de 2022, así como de la aplicación de controles sobre los activos de información y los requerimientos del Modelo de Seguridad y Privacidad de la Información (MSPI) que esta sociedad realice a través de la Oficina de Tecnologías e Información.

ARTÍCULO NOVENO. En cumplimiento de lo establecido en el artículo quinto, en relación con el uso de los sistemas o herramientas de Información por parte de los servidores públicos, contratistas o terceros que laboran en la Sociedad Tequendama, éstos son responsables de la protección de la información que acceden y procesan, así como de evitar su pérdida, alteración, destrucción y uso indebido. Por tal motivo el Grupo de Talento Humano, y los supervisores de los contratos, deberán reportar inmediatamente cualquier tipo de novedad que presenten los servidores públicos, contratistas o terceros a la Oficina de Tecnología.

9. INDICADORES

Objetivo. Medir la efectividad, eficiencia y eficacia del Modelo se Seguridad y Privacidad de la Información y generar las mejoras en el mismo

- Evaluar la efectividad de la implementación de los controles de seguridad
- Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.
- Comunicar valores de seguridad al interior de la entidad.
- Servir como insumos al plan de análisis y tratamiento de riesgos.

iNDICADOR	ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN.	CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN.	TRATAMIENTOS DE EVENTOS RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Definición	El indicador permite determinar y hacer seguimiento, al compromiso de la dirección, en cuanto a seguridad de la información, en lo relacionado con la asignación de personas y responsabilidades relacionadas a la seguridad de la información al interior de la entidad	El indicador permite determinar y hacer seguimiento al cubrimiento que se realiza a nivel de activos críticos de información de una entidad y los controles aplicados.	El indicador permite determinar la eficiencia en el tratamiento de eventos relacionados la seguridad de la información. Los eventos serán reportados por los usuarios o determinadas en las auditorías planeadas para el sistema.
Objetivo	Hacer un seguimiento a la asignación de recursos y responsabilidades en gestio de seguridad de la información, por parte de la alta dirección.	Hacer un seguimiento a la inclusión de nuevos activos críticos de información y su control, dentro del marco de seguridad y privacidad de la información.	El objetivo del indicador es reflejar la gestión y evolución del modelo de seguridad y privacidad de la información al interior de una entidad
Variables	A: Numeros de personas con su respectivo rol B: Numero de personas con su respeivo rol definio despues de un año	VSI03: Número de activos críticos de información incluidos en el alcance de implementación del modelo, incluidos en la zona de riesgo inaceptable y la implementación del control no requiere adquisición de elementos de hardware o software. VSI04: Número de activos críticos de información incluidos en el alcance de implementación del modelo; activos incluidos en la zona de riesgo inaceptable	VSI05: Número de anomalías cerradas VSI06: Número total de anomalías encontradas.
Formula	(A / B)*100	(VSI03/VSI04)*100	(VSI05/VSI06)*100
Fuente de informacion	Capitulo 2. guía del modelo de operación del marco de seguridad y privacidad de la información. Guía No.4 Roles y responsabilidades MSPI DOMINIOS: 1. Servcicios tecnologicos, 2. Estrategia TI 3. Gobierno TI 4. Sistema de informaciòn 5. Uso y apropiacion EQUIPO por Directivos y representante areas misionales "Asegurar que sea una iniciativa de caracter transversal a la entidad y no que dependa exclusivamente de la oficina o area de TI". 1. Personal de seguridad de la información 2. Representante del area de TI 3. Representante del area de Control Interno 4. Representante del area de Planeaciòn 5. Representante del area de Sistema Gestion de calidad 6. Representante del area Juridica 7. Funcionarios, proveedores y ciudadanos	Alcance del SGSI, Inventario de Activos de información, plan de tratamiento, matriz de riesgos. Inventario de Activos de información, nuevos Responsables de la Seguridad de la Informacion (pnto anterior) Guía para la Gestion y Clasificaciòn de Activos de Informacion: Inventario de Activos Propiedad e los activos Clasificaciòn: 1. Confidencialidad 2. Integridad 3. Disponibilidad Etiquetado de Activos de informaciòn Gestionde activos 1. inventario 2. propiedad 3. uso aceptable de los activos 4. devolucion de activos 5. clasifiacion de la infomacion 6. Etiquetado de la informacion 7. Manejo de activos	Auditorías internas, herramientas de monitoreo *Auditor: Asesor dentro de la entidad (organigrama) Guía No.15 Auditoria: Planeaciòn Implementacion Monitoreo Audtoria Informatica Audtoria de Sistemas Metricas