PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2023-2026

TABLA DE CONTENIDO

Contenido

INTRODUCCION 3

1. OBJETIVO 4

1.1 Objetivos Específicos 4

2. ALCANCE 4

3. DEFINICIONES 4

4. MARCO NORMATIVO 5

5. CONOCIMIENTO DE LA ENTIDAD 6

6. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 8

7. MODELO SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 8

8. PLAN DE IMPLEMENTACION DEL MODELO DE SEGURIDAD DE LA INFORMACION. 12

INTRODUCCION

El presente documento describe el Plan de Seguridad y Privacidad de la Dirección de Veteranos y Rehabilitación Inclusiva - DIVRI, alineado con los objetivos, metas, procesos, procedimientos y estructura organizacional de la Entidad, de acuerdo a lo establecido en los lineamientos de la Política de Gobierno Digital, sus componentes, y habilitadores transversales.

El habilitador de Seguridad y Privacidad, permite a la Dirección de Veteranos y Rehabilitación Inclusiva - DIVIR garantizar la confidencialidad, disponibilidad e integridad de la información, de acuerdo al modelo de seguridad establecido por MINTIC, y alienado a las directivas y políticas del sector Defensa.

1. OBJETIVO

Establecer las actividades contempladas en el Modelo de Seguridad y Privacidad de la Información – MSPI de la política de Gobierno Digital del MinTIC, alineadas con la NTC/IEC ISO 27001 y los criterios de Continuidad de la operación de los servicios, que permitan mantener la seguridad y privacidad de la información que circula en los procesos de la DIVRI.

1.1 Objetivos Específicos

- Incrementar el nivel de madurez en la gestión de la seguridad de la información.
- Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad en la entidad.
- Establecer lineamientos para la metodología de gestión de activos de información acorde a los requerimientos mínimos del MINTIC y DAFP.
- 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.
- 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.

2. ALCANCE

El plan de seguridad y privacidad de la información será aplicado a los procesos estratégicos, misionales, de apoyo, y control de la DIVRI, por tal motivo, deberá ser conocido y cumplido por todas las partes interesadas, que accedan a los sistemas de información, repositorios digitales, e instalaciones físicas..

3. 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).
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 auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (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.
Amenaza. causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.
Amenaza informática. la aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado (Ministerio de Defensa de Colombia).
Análisis de riesgos. proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.
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).
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).
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 CRC2258 de2009).
Ciberseguridad. capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética

4. MARCO NORMATIVO

Ley 527de 1999. Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.
Ley 594 de 2000. Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.
Ley 1266 de 2008. Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países información

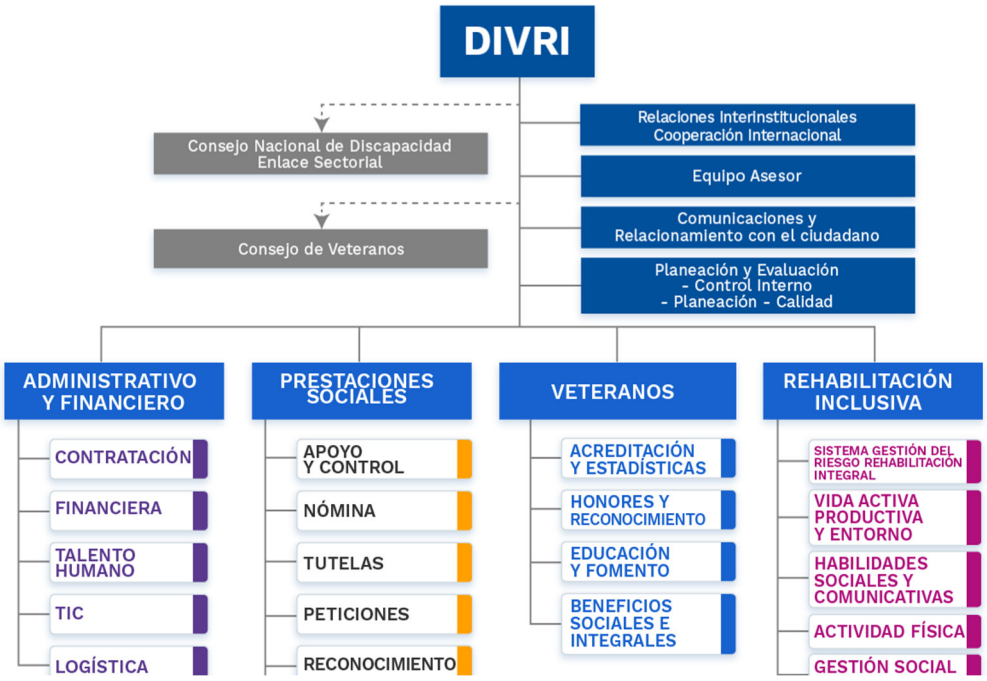
Ley 1273 de 2009. Por medio de la cual se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.
Ley 1581 de 2012. Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.
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.
Decreto 1499 de 2017. Modelo Integrado de Planeación y Gestión y Manual operativo.
Decreto 1008 de 2018. Establece los lineamientos generales de la política de Gobierno Digital. Deroga el Decreto 2573 de 2014.
Normas Técnicas colombianas - NTC/IEC ISO 27001:2013

5. CONOCIMIENTO DE LA ENTIDAD

Misión
La Dirección de Veteranos y Rehabilitación Inclusiva, es una dependencia del Ministerio de Defensa Nacional, con autonomía administrativa y financiera, que busca satisfacer las necesidades y expectativas dentro del marco normativo vigente, para la población de veteranos y demás poblaciones definidas por ley que sean responsabilidad de la Dirección, a través del diseño e implementación de políticas y lineamientos, prestación de servicios y trámites en materia de reconocimiento, bienestar, representación, rehabilitación inclusiva y procesos prestacionales.

Visión
En 2032 la Dirección de Veteranos y Rehabilitación Inclusiva será reconocida a nivel nacional e internacional como la dependencia del Ministerio de Defensa Nacional líder en innovación, transparencia y efectividad en el diseño e implementación de políticas y lineamientos, así como la prestación de servicios y trámites con calidad y calidez, definidos para los veteranos y demás poblaciones establecidas por ley.

ORGANIGRAMA:



MAPA DE PROCESO

La UESVALLE, cuenta con el proceso TICS, el cual tiene a cargo los procedimientos, manuales, formatos y todo el tema documental correspondiente a seguridad y privacidad de la información.

6. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La política de seguridad y privacidad de la información se encuentra en proceso d revisión y aprobación por parte de Alta dirección de la DIVRI, por lo que durante esta vigencia se apoyaran esfuerzos para realizar su socialización e implementación.

7. MODELO SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El modelo del MSIP se encuentra basado en el ciclo de mejoramiento continuo PHVA (Planear, hacer, actuar y verificar), el cual asegura que esté expuesto a revisiones continuas cuando existe un cambio importante en la infraestructura o se requiera mejorar su efectividad dependiendo de las mediciones de parámetros claves de su operación. Se cuenta, entonces, con un ciclo que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar.

Figura 1. **Ciclo de operación Modelo de Seguridad y Privacidad de la Información**
Fuente: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

7.1 Fase
I – Diagnostico y Situación Actual

De acuerdo al modelo de seguridad y privacidad, se establece para la vigencia 2020 las siguientes metas:

Metas	Actividades
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la DIVRI	Diagnóstico de la situación actual de la entidad con relación a la gestión de seguridad de la información. Valoración estado actual de la gestión de seguridad de la entidad con base en el Instrumento de Evaluación MSPI de MINTIC.
Identificar el nivel de madurez de seguridad y privacidad de la información en la DIVRI	Valoración del nivel de madurez de seguridad y privacidad de la información en la DIVRI de acuerdo con los lineamientos establecidos en el capítulo 'MODELO DE MADUREZ' del documento Modelo de Seguridad y Privacidad de la Información de la estrategia
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Ejecución prueba de vulnerabilidades con el fin de identificar el nivel de seguridad y protección de los activos de información de la entidad y definición de planes de mitigación.

7.1.1 Autodiagnóstico de Seguridad Y Privacidad De La Información Año 2022

A continuación, se presenta el resultado del autodiagnóstico realizado en la DIVRI, durante la vigencia 2022.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	22	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	9	100	INICIAL
A.8	GESTIÓN DE ACTIVOS	0	100	INEXISTENTE
A.9	CONTROL DE ACCESO	100	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	100	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	100	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	100	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	100	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	100	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	100	INEXISTENTE
A.18	CUMPLIMIENTO	5	100	INICIAL
PROMEDIO EVALUACIÓN DE CONTROLES		51	100	EFECTIVO

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2022	Planificación	7%	40%
	Implementación	3%	20%
	Evaluación de desempeño	0%	20%
	Mejora continua	0%	20%
TOTAL		10%	100%

Último libro guardado: Ahora mismo

De acuerdo con estos resultados, se continúa la etapa de planificación de acuerdo con el Modelo de Seguridad.

7.2 Fase II- Planificación

Durante la vigencia 2023, se continúa con la fase de planeación la cual permite definir la estrategia metodológica, el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad de la información, en procura de los resultados que permitan dar cumplimiento con las metas propuestas, a continuación, los documentos desarrollados para tal fin:

Metas	Actividades
Política de Seguridad y Privacidad de la Información.	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.
Procedimientos de seguridad de la información	Procedimientos, debidamente documentados, socializados y aprobados por Calidad.
Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección.
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.

7.3 Fase III- Implementación

Durante la vigencia 2024, se llevará a cabo la implementación de la fase II de planeación, teniendo en cuenta para esto los aspectos más relevantes en los procesos de implementación del Sistema de Gestión de Seguridad de la Información de la DIVRI.

7.4 Fase IV- Evaluación

Durante la vigencia 2025, se realizará el proceso de evaluación y cumplimiento de los planes de acuerdo a los instrumentos e indicadores de resultados que permitan determinar la efectividad de la implementación del SGSI.

Metas	Actividades
Plan de revisión y seguimiento, a la implementación del MSPI.	Establecer tablero de mando e indicadores de cumplimento de los planes de PSPSI y PTRPSI.
Plan de Ejecución de Auditorias.	Documento con el informe por parte de Calidad, con los resultados de la auditoría interna. Socializado a la Alta Dirección.

7.5 Fases V - Mejora Continua

Para la vigencia 2026 se consolidarán los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el modelo de seguridad.

Metas	Actividades
Plan de mejora continua.	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados

8. PLAN DE IMPLEMENTACION DEL MODELO DE SEGURIDAD DE LA INFORMACION.

El plan de implementación para la dimensión de seguridad y privacidad de la información establece el siguiente cronograma el cual tendrá seguimiento de manera trimestral.

FASES	Linea de Base - 2023	2024	2025	2026
FASE I -Diagnóstico	x			
FASE II -Planificación	x	x		
FASE III –Implementación		x	x	
FASE IV –Evaluación			x	
FASE V –Mejora Continua				x

A continuación, se detalla las actividades a desarrollar en la vigencia 2023, y cada año se proyectará las actividades siguientes actualizando solo la versión de este plan.

8.1 Cronograma de Actividades Año 2023

Gestión	Actividades	Responsable de la Tarea	Fecha Inicio	Fecha Final
Activos de Información	Elaborar el inventario de activos de seguridad y privacidad de la información de la entidad, clasificarlo de acuerdo con los criterios de disponibilidad, integridad y confidencialidad,	TICS	31/03/2023	30/06/2023
Gestión de Riesgos	Elaborar la política y metodología de gestión de riesgos	TICS	01/07/2023	30/09/2023

	de seguridad digital.			
Gestión de Monitoreo	Definir indicadores para medir la eficiencia y eficacia del sistema de gestión de seguridad y privacidad de la información (MSPI) de la DIVRI	TICS	01/10/2023	31/12/2023

8.2 Proyección de presupuesto PSPSI

La proyección estimada de presupuesto para la ejecución del PSPSI, se encuentra alineado con el PETI para cumplir con el Plan de Estratégico de la DIVRI 2023 así:

PRESUPUESTO 2023	
SERVICIO INFRAESTRUCTURA TECNOLOGICA	**VALOR**
Soporte y Mantenimiento Software	541.324.320
Renovación de Licencias Software	790.000.000
Redes y seguridad	127.678.850
Conectividad	220.510.570
Mantenimiento Preventivo y Correctivo	121.240.000