Plan

DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GTE-PL-02-V6

Gestión tecnológica
UNIDAD NACIONAL DE PROTECCIÓN
29-01-2024

COLOMBIA POTENCIA DE LA VIDA

Tabla de contenido

1. OBJETIVO 3
2. ALCANCE 3
3. DEFINICIONES. 3
4. MARCO LEGAL 5
5. CONDICIONES GENERALES 6
6. CONTENIDO 7
   - *6.1 Estrategias* 7
   - *6.2 Proyectos* 7
   - *6.3 Acciones* 7
   - *6.4 SITUACIÓN ACTUAL* 8
   - *6.4.1 METODOLOGIA UTILIZADA* 8
7. INDICADOR 13
8. DOCUMENTOS RELACIONADOS. 13
9. ANEXOS. 13
10. CONTROL DE CAMBIOS 13
11. CRÉDITOS 14

1. OBJETIVO

Establecer las actividades definidas por el Modelo de Seguridad y Privacidad de la Información MSPI, alineadas con la NTC/IEC ISO 27001:2013, las políticas específicas de seguridad de la información y Continuidad del Negocio dentro del Sistema Integrado de la Unidad Nacional de Protección – UNP.

2. ALCANCE

El Modelo de Seguridad y Privacidad de la Información – MPSI, está estructurado en la norma NTC/IEC ISO 27001:2013 que define los requisitos del Sistema de Gestión de Seguridad de la información - SGSI. Por ser éste un sistema de gestión, su proceso de implementación incluye las actividades del ciclo de Deming PHVA, por lo tanto, la implementación del modelo inicia con las actividades del Planear y termina con las actividades del actuar, que corresponden al mejoramiento continuo e involucra a todos los niveles de la Unidad Nacional de Protección – UNP, incluyendo servidores públicos, contratistas, proveedores, operadores, personas y/o terceros que en razón del cumplimiento de sus funciones y las de la UNP compartan, utilicen, recolecten, procesen, intercambien o consulten información institucional, así como a los Entes de Control y entidades relacionadas que accedan, interna o externamente a cualquier información de la Unidad Nacional de Protección.

3. DEFINICIONES.

ACTIVOS 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. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

AMENAZA: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (Norma ISO 27000).

ANÁLISIS DE RIESGOS: uso sistemático de la información para identificar las fuentes y estimar el riesgo. (Norma ISO 27000).

AUTENTICIDAD: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

CAUSA: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

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. (CONPES 3701).

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (Norma ISO 27000).

CONTROL: Medida por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguardan o contramedida son utilizados frecuentemente como sinónimos de control. (Norma ISO 27000).

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (Norma ISO 27000).

IMPACTO: Cambio adverso en el nivel de los objetivos del negocio logrados. (Norma ISO 27005).

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (Norma ISO 27000).

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud. Fuente: (Norma ISO 27000).

RIESGO DE SEGURIDAD DE LA INFORMACIÓN: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información. Seguridad de la información: preservación de la confidencialidad, integridad, y disponibilidad de la información. (Norma ISO 27000).

RIESGO INHERENTE: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

RIESGO RESIDUAL: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

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. (Norma ISO 27000).

SEGURIDAD DE LA INFORMACIÓN: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (*Accountability*), no repudio y fiabilidad: (Norma ISO 27000).

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI: parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. (Norma ISO 27000).

SOFTWARE MALICIOSO: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse en un computador o una red para dañar recursos informáticos, sistemas operativos, redes de datos o sistemas de información.

TECNOLOGÍA DE LA INFORMACIÓN: Conjunto de hardware y software operados por la entidad o por un tercero en su nombre, que componen la plataforma necesaria para procesar y administrar la información que requiere la entidad para llevar a cabo sus funciones.

VULNERABILIDAD: debilidad de un activo o control que puede ser explotada por una o más amenazas. (Norma ISO 27000).

4. MARCO LEGAL

- Constitución Política de Colombia art 15, 20, 23 y 74.
- Ley 2294 de 2023, por la cual se expide el Plan Nacional de Desarrollo 2022-2026 "Colombia potencia mundial de la vida"
- Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014 "Ley de transparencia y del derecho de acceso a la información pública nacional"
- Decreto 338 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.
- Decreto 767 de 2022. 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.
- 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.
- Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- 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"
- Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL hoy Gobierno Digital.
- Resolución 1519 de 2020, "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos"
- Norma Técnica Colombiana NTC-ISO/IEC 27001 Sistemas de Gestión de la Seguridad de la Información.
- Norma Técnica Colombiana NTC-ISO/IEC 27002 Tecnología de la Información. Técnica de Seguridad. Código de Práctica para Controles de Seguridad de la Información.
- Norma Técnica Colombiana NTC-ISO/IEC ISO 27005 Tecnología de la Información

  Técnicas de Seguridad. Gestion del Riesgo de la Seguridad de la Información. Decreto 103 de 2015, Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
- Decreto 1494 de 2015, Por el cual se corrigen yerros en la Ley 1712 de 2014
- 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 2573 de 2014, Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
- CONPES 3995 de 2020. Confianza y Seguridad Digital
- CONPES 3854 de 2017. Política Nacional de Seguridad digital.
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- Política de Seguridad de la Información de la Entidad. Resolución 0199 del 2 de marzo de 2020

5. CONDICIONES GENERALES

El presente documento está enmarcado en las directrices contenidas en Modelo de Seguridad y Privacidad de la Información MSPI, alineadas con la NTC/IEC ISO 27001:2013 y la Política de Seguridad Digital de MINTIC y busca establecer los lineamientos de implementación de las acciones para la seguridad y privacidad de la información.

6. CONTENIDO

6.1 Estrategias

La Unidad Nacional de Protección – UNP, a través de la adopción e implementación con el Sistema de Gestión de Seguridad de la Información, enmarcado en el Sistema de Gestión de Seguridad de la información - SGSI, tiene como objeto proteger, preservar y administrar la confidencialidad, integridad y disponibilidad de la información, mediante una gestión integral de riesgos y la implementación de seguridad de la información reduciendo la probabilidad de ocurrencia de 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 del Sistema de seguridad de la Información las .

Para lograr el cumplimiento del presente plan se definen las siguientes estrategias el uso aceptable y preservación y conservación de los activos físicos y de información definidos en la entidad:

1. Mitigar los impactos y reducir la ocurrencia de posibles incidentes de Seguridad de la Información, de forma efectiva, eficaz y eficiente.
2. Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad de la información de la UNP.
3. Definir los lineamientos necesarios para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad de la Información.
4. Generar conciencia para el cambio organizacional requerido para la apropiación eficaz de la Seguridad de la Información como eje transversal en la UNP.
5. Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información.

6.2 Proyectos

A continuación, se presentan, los proyectos propuestos para dar cumplimiento a la aplicación del MSPI, los cuales se deberán analizar de acuerdo con las directrices, capacidades, aprobaciones y apoyo de la alta dirección para su ejecución:

1. Apoyo a la gestión documental para el levantamiento de activos de información
2. Mejora continua y matenimiento del Sistema de Gestión de Seguridad de la información - SGSI.
3. Fortalecimiento, uso y apropiación de herramientas de control y restricción para la seguridad de la información.
4. Fortalecimiento de la arquitectura de seguridad informática a través de plataformas especializadas.

6.3 Acciones

Las acciones listadas en Tabla 1, son las requeridas para dar cumplimiento a los objetivos propuestos del plan de seguridad y privacidad de la información de acuerdo con el estado

actual de la Entidad, definiendo actividades, productos, responsables a partir del cual se establece el cronograma de ejecución el cual se encuentra en los Anexos de este documento.

6.4 SITUACIÓN ACTUAL

La situación actual se entiende el nivel de madurez que posee en este momento la Unidad Nacional de Protección UNP con relación a la seguridad de la información. El proceso por el cual se lleva a cabo esta estimación del nivel de madurez se denomina Instrumento de diagnóstico del MSPI de Mintic. Para poder realizar el Plan Estratégico de Seguridad de la Información PESI es necesario considerar los niveles de madurez alcanzados por cada uno de los dominios (ver tabla a continuación) con el fin de plantear prioridades sobre su implementación.

Tabla Nivel de Madurez MSPI - UNP

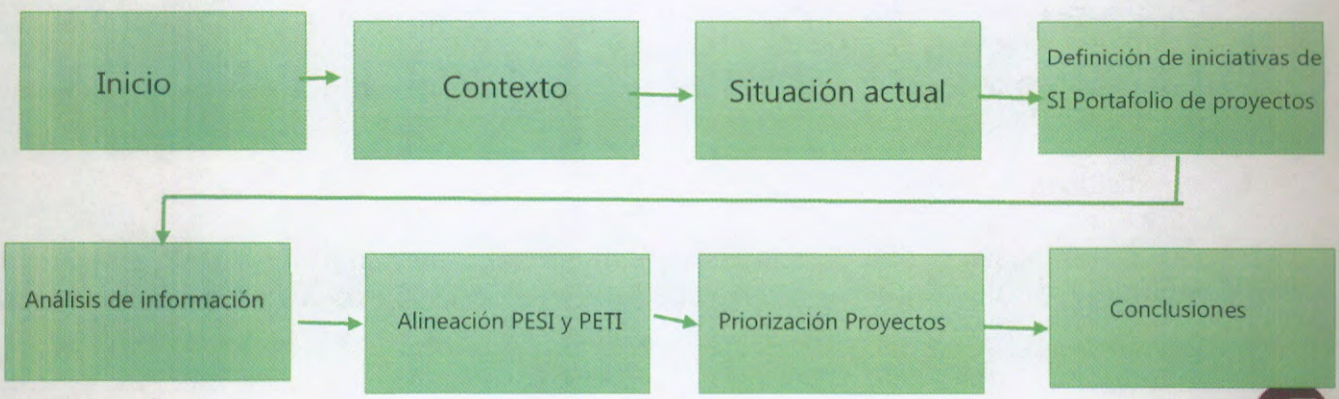
DOMINIO	ESPERADO	PUNTAJE
A.5 Políticas de Seguridad de la Información	10	8
A.6 Organización de la Seguridad de la Información	10	6
A.7 Seguridad de los Recursos Humanos	10	5
A.8 Gestión de Activos	10	4
A.9 Control de Acceso	10	5
A.10 Criptografía	10	4
A.11 Seguridad Física y del Entorno	10	6,66
A.12 Seguridad de las Operaciones	10	4
A.13 Seguridad de las Comunicaciones	10	2
A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas	10	4
A.15 Relaciones con los Proveedores	10	3
A.16 Gestión de Incidentes de Seguridad de la Información	10	4
A.17 Gestión de Continuidad del Negocio	10	3
A.18 Cumplimiento	10	6

Fuente Elaboración Propia

6.4.1 METODOLOGIA UTILIZADA

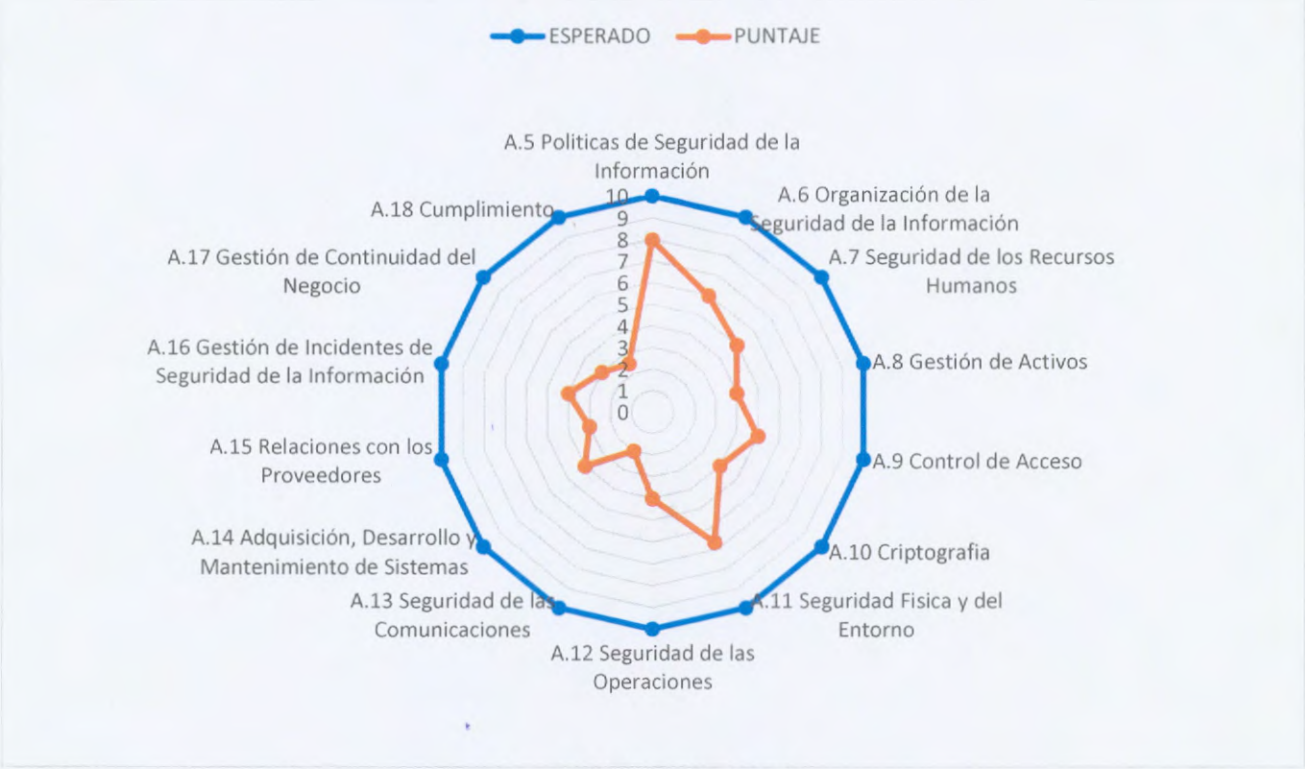
La metodología utilizada para el desarrollo del PESI se muestra y se explica a continuación:

Ilustración. Metodología Utilizada



La madurez permite establecer las bases para mejorar el proceso de Seguridad de la Información de la UNP e identificar las iniciativas de seguridad de la información, que deben alinearse a las necesidades identificadas en el Plan Estratégico de Tecnologías de Información y Comunicaciones y la estrategia de información (PETI). En seguida, se presenta el nivel de madurez del modelo de seguridad y privacidad de la información y el porcentaje de cumplimiento de la Entidad frente a los 14 dominios de la norma ISO/IEC 27001:2013 y ISO/IEC 27002:2013

Ilustración Nivel de Madurez MSPI - UNP



Fuente Elaboración Propia

Tabla : Acciones Plan de Seguridad y Privacidad de la Información 2024

Capítulo	Actividad	Producto	Responsable
Revisión	Revisar los resultados del SGSI	Resultados para la preparación certificación bajo el estándar ISO 27001.2022	Coordinador GGT, contratistas de seguridad, auditor y OAPI
Revisión	Revisar los resultados de Evaluación de Nivel de Madurez del SGSI.	Resultados de Madurez para la preparación certificación bajo el estándar ISO 27001.2022	Coordinador GGT, contratistas de seguridad, auditor y OAPI
Mejora	Identificar oportunidades de mejora al SGSI.	Remediación para la preparación certificación bajo el estándar ISO 27001.2022	Coordinador GGT, contratistas de seguridad, auditor y OAPI
Identificación de riegos	Identificación y uso aceptable de activos físicos y de Información	Listado de activos físicos y de Información	Coordinador GGT, contratistas de seguridad, auditor y OAPI
Evaluación de Riesgos	Metodología de evaluación de riesgos	Informe de monitoreo y aceptación del plan de tratamiento de riesgos de seguridad de la información	Coordinador GGT, contratistas de seguridad, auditor y OAPI
Políticas y Procedimientos	Contexto de la organización	Identificación del contexto de la organización (partes interesadas, alcance y políticas)	Coordinador GGT, contratistas de seguridad, auditor y OAPI
	Comprensión de las necesidades y expectativas de las partes interesadas	Identificación de las partes interesadas, sus necesidades y expectativas relacionadas con la seguridad de la información	Coordinador GGT, contratistas de seguridad, auditor y OAPI
	Determinación del alcance del sistema de gestión de seguridad de la información	Definición del alcance del SGSI	Coordinador GGT, contratistas de seguridad, auditor y OAPI
Control de Acceso	Liderazgo y compromiso	Establecimiento de una política de seguridad de la información	Coordinador GGT, contratistas de seguridad, auditor y OAPI
		Asignación de roles y responsabilidades para la seguridad de la información	Coordinador GGT, contratistas de seguridad, auditor y OAPI
	Política de seguridad de la información	Desarrollo y aprobación de la política de seguridad de la información	Coordinador GGT, contratistas de seguridad, auditor y OAPI

Capítulo	Actividad	Producto	Responsable
Protección de Datos	Gestión de riesgos	Identificación y evaluación de riesgos de seguridad de la información	Coordinador GGT, contratistas de seguridad, auditor y OAPI
		Establecimiento de controles de seguridad adecuados para mitigar los riesgos	Coordinador GGT, contratistas de seguridad, auditor y OAPI
		Elaboración del plan de tratamiento de riesgos	Coordinador GGT, contratistas de seguridad, auditor y OAPI
Sensibilización y Capacitación	Soporte	Identificación de recursos necesarios para el SGSI	Coordinador GGT, contratistas de seguridad, auditor y OAPI
		Capacitación y concientización sobre seguridad de la información	Coordinador GGT, contratistas de seguridad, auditor y OAPI Recursos Humanos
		Establecimiento de procedimientos documentados	Coordinador GGT, contratistas de seguridad, auditor y OAPI
Monitoreo y Detección	Operación	Implementación de controles de seguridad (acceso, cifrado, monitoreo)	Coordinador GGT, contratistas de seguridad, auditor y OAPI
Monitoreo y Detección	**Operación**	Gestión de cambios y control de versiones de los activos de información	Coordinador GGT, contratistas de seguridad, auditor y OAPI
Gestión de Incidentes	Evaluación del desempeño	Monitoreo y medición del desempeño del SGSI	Coordinador GGT, contratistas de seguridad, auditor y OAPI
		Realización de auditorías internas	Coordinador GGT, contratistas de seguridad, auditor y OAPI

Capítulo	Actividad	Producto	Responsable
Revisión y Mejora Continua	Mejora	Implementación de acciones correctivas y preventivas	Coordinador GGT, contratistas de seguridad, auditor y OAPI
Revisión de mejora continua		Revisión de la efectividad del SGSI por la dirección	Coordinador GGT, contratistas de seguridad, auditor y OAPI
Revisión	Revisar del SGSI por la Dirección.	Resultados para la preparación certificación bajo el estándar ISO 27001.2022	Coordinador GGT, contratistas de seguridad, auditor y OAPI
Mejora	Identificar oportunidades de mejora al SGSI.	Remediación para la preparación certificación bajo el estándar ISO 27001.2022	Coordinador GGT, contratistas de seguridad, auditor y OAPI
Certificación	Plantear la necesidad de certificación de los procesos de la UNP bajo el estándar ISO 27001.2022	Preparación certificación bajo el estándar ISO 27001.2022	Coordinador GGT, contratistas de seguridad, auditor y OAPI

Fuente: Elaboración propia.

Anexos

CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - 2024

Gestión tecnológica
UNIDAD NACIONAL DE PROTECCIÓN
29-01-2024

COLOMBIA POTENCIA DE LA VIDA

Cronograma Plan de Seguridad y Privacidad de la Información 2024

Capítulo	Actividad	Producto	Responsable	Fecha Inicio	Fecha cumplimiento	Trimestre de reporte
Revisión	Revisar los resultados de Evaluación de Nivel de Madurez del SGSI.	Resultados de Madurez para la preparación certificación bajo el estándar ISO 27001.2022	Coordinador GGT, contratistas de seguridad, auditor y OAPI	20/1/2024	30/3/2024	I trimestre
Mejora	Identificar oportunidades de mejora al SGSI.	Remediación para la preparación certificación bajo el estándar ISO 27001.2022	Coordinador GGT, contratistas de seguridad, auditor y OAPI	10/03/2024	30/06/2024	I y II trimestre
Identificación de riegos	Identificación y uso aceptable de de activos físicos y de Información	Listado de activos físicos y de Información	Coordinador GGT, contratistas de seguridad, auditor y OAPI	1/06/2024	30/09/2024	III trimestre
Evaluación de Riesgos	Metodología de evaluación de riesgos	Informe de monitoreo y aceptación del plan de tratamiento de riesgos de seguridad de información Evaluación de Riesgos.	Coordinador GGT, contratistas de seguridad, auditor y OAPI	2/02/2024	30/6/2024	I y II trimestre
Políticas y Procedimientos	Contexto de la organización	Identificación del contexto de la organización (partes interesadas, alcance, y políticas)	Coordinador GGT, contratistas de seguridad, auditor y OAPI	10/03/2024	30/06/2024	I y II trimestre
	Comprensión de las necesidades y expectativas de las partes interesadas	Identificación de las partes interesadas, sus necesidades y expectativas relacionadas con la seguridad de la información	Coordinador GGT, contratistas de seguridad, auditor y OAPI	10/03/2024	30/06/2024	I y II trimestre
	Determinación del alcance del sistema de gestión de seguridad de la información	Definición del alcance del SGSI	Coordinador GGT, contratistas de seguridad, auditor y OAPI	1/06/2024	30/09/2024	III trimestre
Control de Acceso	Liderazgo y compromiso	Establecimiento de una política de seguridad de la información	Coordinador GGT, contratistas de seguridad, auditor y OAPI	01/01/2024	31/03/2024	I trimestre de 2024
		Asignación de roles y responsabilidades para la seguridad de la información	Coordinador GGT, contratistas de seguridad, auditor y OAPI	01/01/2024	31/03/2024	I trimestre de 2024

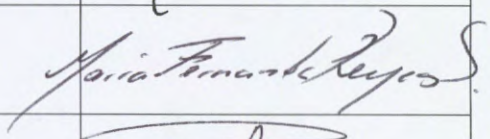
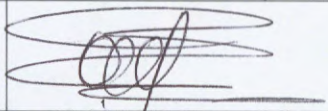
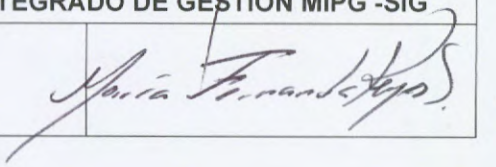
Capítulo	Actividad	Producto	Responsable	Fecha Inicio	Fecha cumplimiento	Trimestre de reporte
	Política de seguridad de la información	Desarrollo y aprobación de la política de seguridad de la información	Coordinador GGT, contratistas de seguridad, auditor y OAPI	01/06/2024	31/9/2024	III trimestre de 2024
Sensibilización	Política de seguridad	Crear conciencia y empoderamiento	Coordinador GGT, contratistas de seguridad, auditor y OAPI	01/09/2024	30/12/2024	III y IV trimestre 2024
Protección de Datos	Gestión de riesgos	Identificación y evaluación de riesgos de seguridad de la información	Coordinador GGT, contratistas de seguridad, auditor y OAPI	01/04/2024	30/06/2024	II trimestre de 2024
		Establecimiento de controles de seguridad adecuados para mitigar los riesgos	Coordinador GGT, contratistas de seguridad, auditor y OAPI	01/04/2024	30/06/2024	II trimestre de 2024
		Elaboración del plan de tratamiento de riesgos	Coordinador GGT, contratistas de seguridad, auditor y OAPI	01/04/2024	30/06/2024	II trimestre de 2024
Sensibilización y Capacitación	Soporte	Identificación de recursos necesarios para el SGSI	Coordinador GGT, contratistas de seguridad, auditor y OAPI	01/04/2024	30/06/2024	II trimestre de 2024
		Capacitación y concientización sobre seguridad de la información	Coordinador GGT, contratistas de seguridad, auditor y OAPI Recursos Humanos	01/04/2024	30/08/2024	II y III trimestre de 2024
		Establecimiento de procedimientos documentados	Coordinador GGT, contratistas de seguridad, auditor y OAPI	01/04/2024	30/08/2024	II y III trimestre de 2024
Monitoreo y Detección	Operación	Implementación de controles de seguridad (acceso, cifrado, monitoreo)	Coordinador GGT, contratistas de seguridad, auditor y OAPI	01/04/2024	30/09/2024	II y III trimestre de 2024
		Gestión de cambios y control de versiones de los activos de información	Coordinador GGT, contratistas de seguridad, auditor y OAPI	01/04/2024	30/06/2024	II trimestre de 2024
Gestión de Incidentes	Evaluación del desempeño	Monitoreo y medición del desempeño del SGSI	Coordinador GGT, contratistas de seguridad, auditor y OAPI	01/04/2024	30/06/2024	II trimestre de 2024
		Realización de auditorías internas	Coordinador GGT, contratistas de seguridad, auditor y OAPI	01/04/2024	30/06/2024	II trimestre de 2024

Capítulo	Actividad	Producto	Responsable	Fecha Inicio	Fecha cumplimiento	Trimestre de reporte
Revisión y Mejora Continua	Mejora	Implementación de acciones correctivas y preventivas	Coordinador GGT, contratistas de seguridad, auditor y OAPI	01/04/2024	30/06/2024	II trimestre de 2024
		Revisión de la efectividad del SGSI por la dirección	Coordinador GGT, contratistas de seguridad, auditor y OAPI	1/8/2024	30/11/2024	III y IV trimestre 2024
Revisión	Revisar los resultados del SGSI por la Dirección.	Resultados para la preparación certificación bajo el estándar ISO 27001.2022	Coordinador GGT, contratistas de seguridad, auditor y OAPI	1/8/2424	30/11/2024	III y IV trimestre 2024
Mejora	Identificar oportunidades de mejora al SGSI.	Remediación para la preparación certificación bajo el estándar ISO 27001.2022	Coordinador GGT, contratistas de seguridad, auditor y OAPI	1/8/2424	30/11/2024	III y IV trimestre 2024
Certificación	Plantear la necesidad de certificación de los procesos de la UNP bajo el estándar ISO 27001.2022	Preparación certificación bajo el estándar ISO 27001.2022	Coordinador GGT, contratistas de seguridad, auditor y OAPI	1/8/2424	30/11/2024	III y IV trimestre 2024

Fuente: Elaboración propia.

VERSIÓN INICIAL	DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO	FECHA	VERSIÓN FINAL
02	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2021	20/01/2021	03
03	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2022	20/01/2022	04
04	Actualización de las fechas propuestas en el cronograma de actividades del plan de Seguridad y Privacidad de la Información y desglose de la meta propuesta en el indicador, por valores acumulativos de porcentaje en cada uno de los semestres.	17/05/2022	05
05	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia, se hace claridad en relación a la metodología de trabajo y actualización de las actividades en el cronograma para el Anexo y el plan de Seguridad y Privacidad de la Informaciónn para la vigencia 2024	29/01/2024	06

11. CRÉDITOS

FIRMAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN DEL DOCUMENTO	
Elaboró Nombre: Elsa Marlen Baracaldo Huertas Cargo y/o Vinculación/dependencia: Contratista- Proceso Gestión tecnológica / Oficina Asesora de Planeación e Información	
Revisó: Nombre: Maria Fernanda Reyes Sarmiento Cargo: Jefe de la Oficina Asesora de Planeación e Información	
Aprobó: Nombre: Augusto Rodríguez Ballesteros Cargo: Director General	
FIRMA DE OFICIALIZACIÓN DEL DOCUMENTO- SISTEMA INTEGRADO DE GESTIÓN MIPG -SIG	
Oficializó: Nombre: Maria Fernanda Reyes Sarmiento Cargo: Jefe de la Oficina Asesora de Planeación e Información	

7. INDICADOR

El indicador del plan es el seguimiento al cumplimiento de las actividades y se formula de la siguiente manera, formulado así:

Indicador = ((Actividades ejecutadas en el periodo trimestral) / (actividades programadas en el periodo trimestral)) * 100

Se define meta Base de 85% anual del del Plan de Seguridad y Privacidad de la Información para el periodo 2024.

La meta es acumulativa, desglosándola trimestralmente de la siguiente manera:

TRIMESTRE	PONDERACIÓN DEL TRIMESTRE	META MINIMA DE CUMPLIMIENTO POR TRIMESTRE	META ANUALMINIMA
I TRIMESTRE	25%	20%	85%
II TRIMESTRE	25%	40%	
III TRIMESTRE	25%	60%	
IV TRIMESTRE	25%	85%	

8. DOCUMENTOS RELACIONADOS.

- GDT-FT-23 Acta de Reunión
- DEP-FT-11 Informe de seguimiento a Planes

9. ANEXOS.

- Cronograma de Actividades del Plan de Seguridad y Privacidad de La Información.

10. CONTROL DE CAMBIOS

VERSIÓN INICIAL	DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO	FECHA	VERSIÓN FINAL
00	Creación del Plan Seguridad y Privacidad de la Información	31/01/2019	01
01	Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2020	31/01/2020	02