

**CORPORACION PARA EL DESARROLLO SOSTENIBLE DEL URABA
CORPOURABA**

**MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
MSPI**

**PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN
PESI
2018-2021**

TRD: 300-01 04-05-0225-2018



Apartadó, Julio 24 de 2018

TABLA DE CONTENIDO

Contenido

INTRODUCCIÓN	4
1. OBJETIVO	5
1.1. Objetivos específicos.....	6
2. ALCANCE DEL PESI	6
3. MARCO NORMATIVO	7
4. Política de Seguridad y Privacidad de la Información	8
5. ANÁLISIS DE LA SITUACIÓN ACTUAL	10
5.1 Análisis de brecha MSIP	10
5.1 Análisis de brecha Transición de IPv4 a IPv6.....	13
5.1 Gestión de Información.....	13
6 ANÁLISIS DE RIESGO PARA LA SEGURIDAD DE LA INFORMACIÓN.....	15
7 PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN	15
7.1 Seguridad Del Recurso Humano:.....	15
7.2 Gestión De Activos:	15
7.3 Control De Acceso:	16
7.4 Criptografía: N/A	16
7.5 Seguridad Física Y Del Entorno:.....	16
7.6 Seguridad De Las Operaciones:.....	16
7.7 Seguridad De Las Comunicaciones:.....	16
7.8 Relaciones Con Los Proveedores:.....	16
7.9 Adquisición, Desarrollo Y Mantenimiento De Sistemas De Información:.....	16
7.10 Gestión De Incidentes De Seguridad De La Información:	16
7.11 Aspectos De Seguridad De La Información De La Gestión De Continuidad De Negocio:	17
7.12 Plan de sensibilización y apropiación del MSPI para toda la entidad.	17
8 ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	17
8.1 Gobierno de SI.....	17
Organigrama Corporativo	18
Organigrama de SI	19
8.2 Responsable de Seguridad de la Información:.....	19
8.3 Equipo del Proyecto:	20

**MSPI Y PESI
2018-2021**

9 SEGUIMIENTO Y REVISIÓN DEL MSPI	21
10 PLANIFICACIÓN DE ACTIVIDADES DEL MSPI.....	22
10.1 Proyección de presupuesto área de SI	26
11. Plan de Comunicaciones del PESI.....	28
11.1. Alcance	28
11.2. Red de formadores de formadores.....	29

Jairo Agudelo
Profesional Universitario SPOT

INTRODUCCIÓN

La seguridad de la información, según ISO/IEC 27001:2013, consiste en preservar la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación de un proceso de Gestión de Riesgo, (ISO/ IEC 27001 VERSION 2013, 2013), para lo cual, el proyecto busca dar respuesta a las exigencias que el Ministerio de Tecnologías de la Información y las comunicaciones de Colombia, (MinTic), presenta para todas entidades públicas.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse a los siguientes componentes:

TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

TIC para Gobierno Abierto que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables.

El Plan de Seguridad de la Información (PSI), es un documento que tiene por objetivo trazar y planificar la manera como la entidad realizará o continuará con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

Este plan hace parte del Sistema de Gestión de Seguridad de la Información (SGSI) el cual es una herramienta de la que dispone la gerencia para dirigir y controlar la seguridad de la información.

MSPI Y PESI 2018-2021

Este documento indica, definiendo plazos anuales, cuáles serán las labores que realizará la entidad con el objetivo de lograr el 100% de la implementación del MSPI al interior de todos los procesos de la entidad.

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización. Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

Las actividades para la administración y la seguridad informática pueden clasificarse en varias categorías como son: seguridad funcional, coordinación, documentación, certificación, acreditación, administración de configuraciones de sistemas y de seguridad informática y manejo de riesgos.

Este documento se elabora con el objetivo de orientar a la Corporación para dar cumplimiento con lo solicitado en el Decreto 612 de 2018 y todas las consideraciones expuestas, dentro de las cuáles se encuentra el decreto 1078 de 2015 y los instrumentos para implementar la Estrategia de Gobierno en Línea (Ahora Gobierno Digital), dentro de los cuales se exige la elaboración por parte de cada entidad, de un Plan de Seguridad y Privacidad de la Información.

En el presente documento se adoptó la concepción, metodología, lineamientos e instrumentos desarrollados por el Ministerio de Tecnologías de la Información y las Comunicaciones –MinTIC-, que conforman la Estrategia de Gobierno Digital, la cual está soportada en los LINEAMIENTOS PARA LA ELABORACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN (PESI) ¹ y el MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN².

1. OBJETIVO

¹ LINEAMIENTOS PARA LA ELABORACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN (PESI). Ministerio de Tecnologías de la Información y Comunicaciones, borrador 2018

² MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Ministerio de Tecnologías de la Información y Comunicaciones, borrador 2016.

Liderar y establecer las estrategias para la gestión de seguridad y privacidad de la Información en CORPOURABA que permitan minimizar los riesgos de pérdida de activos de la información y estén alineadas a la estrategia y modelo integrado de gestión y acordes con las necesidades de la Entidad y los lineamientos del programa de Gobierno Digital.

1.1. Objetivos específicos

El PESI³ de la CORPORACIÓN PARA EL DESARROLLO SOSTENIBLE DEL URABA –CORPOURABA- cuenta con los siguientes objetivos específicos acordes con las necesidades de la Entidad y las dimensiones de Gobierno Digital:

- Definir las responsabilidades relacionadas con el manejo de la seguridad, durante el transcurso del año en La Corporación.
- Establecer una metodología de gestión de la seguridad clara y estructurada.
- Reducir el riesgo de pérdida, robo o corrupción de información.
- Garantizar que los usuarios tienen acceso a la información a través medidas de seguridad con la garantía de calidad y confidencialidad.
- Implementar las auditorías externas para identificar las debilidades del sistema y las áreas a mejorar.
- Garantizar la continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Cumplir con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Optimizar la gestión de la seguridad de la información con base en la gestión de procesos.
- Definir el plan para la transición de IPv4 a IPv6 .
- Integración con otros sistemas de gestión (ISO 9001, ISO 14001, SGSST).

2. ALCANCE DEL PESI

El PETI tiene como finalidad el diagnóstico, análisis, definición y planeación del manejo de la seguridad de los procesos que se ejecutan en CORPOURABA y será actualizado anualmente; estos apoyarán el cumplimiento de los procesos y objetivos propuestos por las diferentes

³ Plan Estratégico de las Seguridad de la Información y Comunicaciones (PESI)

dependencias de la Entidad y está articulado de manera global en relación con la seguridad de la información.

3. MARCO NORMATIVO

Ley 527 de 1999: Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones, así mismo introduce el concepto de equivalente funcional, firma electrónica como mecanismos de autenticidad, disponibilidad y confidencialidad de la información. (CONGRESO NACIONAL, 1999).

CONPES 3670 de 2010. "Lineamientos de Política para la continuidad de los programas de acceso y servicio universal a las Tecnologías de la Información y las Comunicaciones".

CONPES 3701 de 2011. "Lineamientos de Política para Ciberseguridad y Ciberdefensa" Ley 872 de 2003. "Por la cual se crea el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios".

Ley 1341 de 2009. "Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones".

Ley 39 de 1981. Sobre microfilmación y certificación de archivos.

Ley 594 de 2000. "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones".

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. (CONGRESO DE LA, 2014)

Decreto 103 de 2015: Por la cual se reglamenta parcialmente la ley 1712 de 2014 y se dictan otras disposiciones, en cuanto a la publicación y divulgación de la información. (PRESIDENCIA DE LA, 2015)

Decreto 2609 de 2012: Por el cual se dictan disposiciones en materia de gestión documental y gestión documental electrónica. (MINISTERIO DE, 2012)

Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones. (MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS, 2012)

Ley 1273 de 2009: Ley la cual se crea y se protege el bien jurídico de la información y los datos personales. (CONGRESO D. C.,

Ley 1581 de 2012: Ley Estatutaria por la cual se reglamenta el artículo 15 de la Constitución política, relativo a la intimidad personal y el Habeas Data, a través de esta norma se dictan disposiciones generales para la protección de datos personales. (CONGRESO D. C., <http://www.alcaldiabogota.gov.co>, 2012).

Ley 594 de 2000: Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. (CONGRESO D. L., 2000)

4. Política de Seguridad y Privacidad de la Información

La Dirección General de la Corporación para el Desarrollo Sostenible del Urabá – CORPOURABA-, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información –SGSI- buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de nuestra Corporación y las políticas de Calidad y del SGSST.

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

El contenido de esta política aplica a la Corporación según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de

decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus usuarios, entes de control y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y usuarios de CORPOURABA
- Garantizar la continuidad de la corporación frente a incidentes.

CORPOURABA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la Corporación, y a los requerimientos regulatorios.

A continuación se establecen las 12 políticas de seguridad que soportan el SGSI de CORPOURABA:

- CORPOURABA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- CORPOURABA protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- CORPOURABA protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- CORPOURABA protegerá su información de las amenazas originadas por parte del personal.

**MSPI Y PESI
2018-2021**

- CORPOURABA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- CORPOURABA controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- CORPOURABA implementará control de acceso a la información, sistemas y recursos de red.
- CORPOURABA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- CORPOURABA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- CORPOURABA garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- CORPOURABA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas

5. ANÁLISIS DE LA SITUACIÓN ACTUAL

5.1 Análisis de brecha MSIP

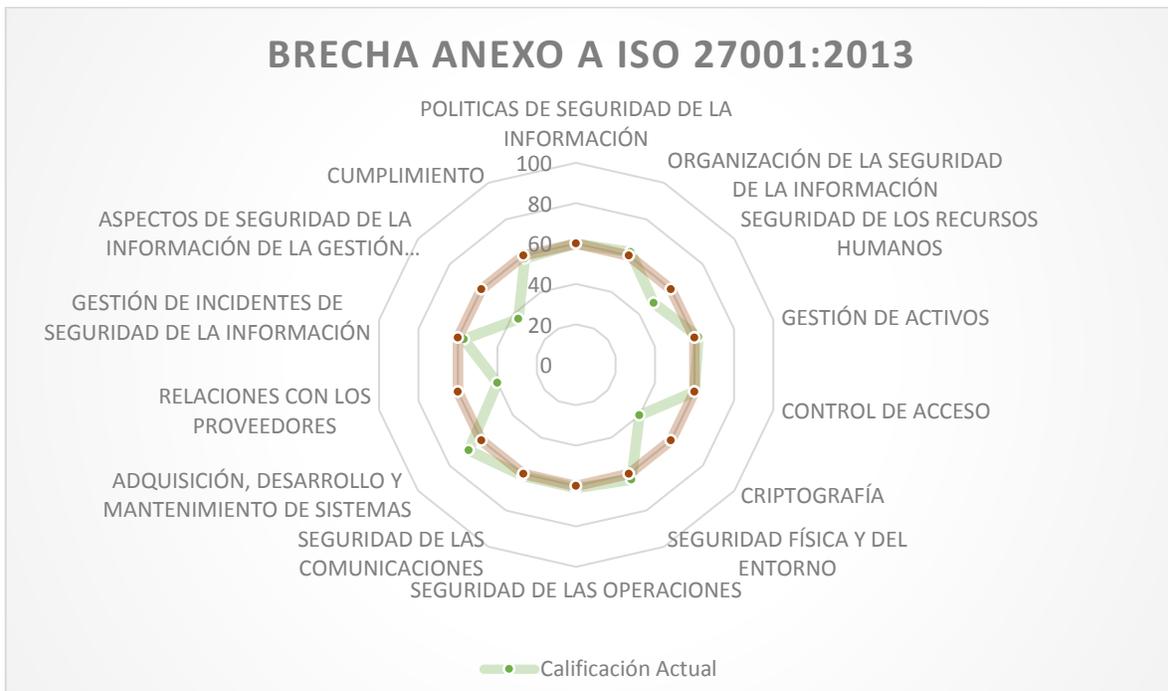
Apyados en la herramienta "INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD" ⁴ se obtuvieron los siguientes resultados de análisis de brecha sobre la efectividad de los controles:

No.	Evaluación de Efectividad de controles			EVALUACIÓN DE EFECTIVIDAD DE CONTROL
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	60	EFFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	62	60	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	49	60	EFFECTIVO
A.8	GESTIÓN DE ACTIVOS	62	60	GESTIONADO

⁴ INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD. Ministerio de Tecnologías de la Información y Comunicaciones, borrador 2017

**MSPI Y PESI
2018-2021**

No.	Evaluación de Efectividad de controles			EVALUACIÓN DE EFECTIVIDAD DE CONTROL
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.9	CONTROL DE ACCESO	60	60	EFFECTIVO
A.10	CRIPTOGRAFÍA	40	60	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	63	60	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	61	60	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	61	60	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	68	60	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	40	60	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	57	60	EFFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	37	60	REPETIBLE
A.18	CUMPLIMIENTO	58,5	60	EFFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		56	60	EFFECTIVO



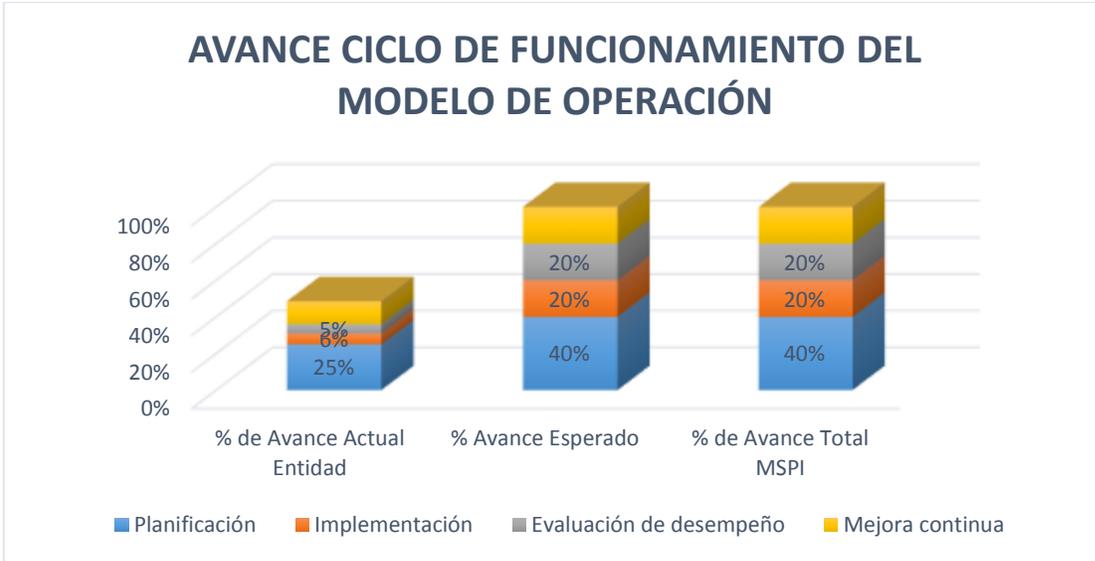
Gracias a este análisis de brecha se identificó que estamos a 4 punto porcentuales de la meta global para el año 2018 y se priorizaron los dominios en naranja y amarillo para el primer año del plan.

En cuanto al análisis de brecha para el avance del PHVA se tiene:

AVANCE PHVA

**MSPI Y PESI
2018-2021**

COMPONENTE	% de Avance Actual Entidad	% Avance Esperado	% de Avance Total MSPI
Planificación	25%	24%	40%
Implementación	6%	12%	20%
Evaluación de desempeño	5%	12%	20%
Mejora continua	13%	12%	20%
TOTAL	49%	60%	100%



Se ha identificado que estamos a 11 puntos porcentuales del logro de la meta del año 2018 y se priorizaron los componentes en amarillo para este año.

En cuanto a la madurez del MSPI se tiene el siguiente análisis.

ID REQUISITO	CALIFICACIÓN OBTENIDA	NIVEL 1 INICIAL	CUMPLIMIENTO NIVEL INICIAL	NIVEL 2 GESTIONADO	CUMPLIMIENTO NIVEL GESTIONADO	NIVEL 3 DEFINIDO	CUMPLIMIENTO NIVEL DEFINIDO	NIVEL 4 GESTIONADO CUANTITATIVAMENTE	CUMPLIMIENTO NIVEL 4 GESTIONADO CUANTITATIVAMENTE	NIVEL 5 OPTIMIZADO	CUMPLIMIENTO NIVEL 5 OPTIMIZADO
BRECHA			OK		R1		R1, R2, R3, R5		R1 a R7		R1 a R8
LÍMITE DE MADUREZ INICIAL	520	260	CUMPLE	440	MENOR	600	MENOR	780	MENOR	980	MENOR
BRECHA			N/A		R9 y R10		R9, R10 y R14		R9 a R19, cumple R13, R17 y R18		R9 a R19
LÍMITE DE MADUREZ GESTIONADO	634	N/A	N/A	460	MENOR	660	MENOR	880	MENOR	1100	MENOR
BRECHA			N/A		N/A		R21, R22, R25,		R20 a R40,		R20 a R40

**MSPI Y PESI
2018-2021**

ID REQUISITO	CALIFICACIÓN OBTENIDA	NIVEL 1 INICIAL	CUMPLIMIENTO NIVEL INICIAL	NIVEL 2 GESTIONADO	CUMPLIMIENTO NIVEL GESTIONADO	NIVEL 3 DEFINIDO	CUMPLIMIENTO NIVEL DEFINIDO	NIVEL 4 GESTIONADO CUANTITATIVAMENTE	CUMPLIMIENTO NIVEL 4 GESTIONADO CUANTITATIVAMENTE	NIVEL 5 OPTIMIZADO	CUMPLIMIENTO NIVEL 5 OPTIMIZADO
							R28, R30, R36, R38, R39 y R40		cumple R24 y R33		
LIMITE DE MADUREZ DEFINIDO	599	N/A	N/A	N/A	N/A	660	MENOR	880	MENOR	1100	MENOR
BRECHA			N/A		N/A		N/A		R41, R50 y R52		R41 a R53
LIMITE DE MADUREZ GESTIONADO CUANTITATIVAMENTE	660	N/A	N/A	N/A	N/A	N/A	N/A	660	MENOR	880	MENOR
BRECHA			N/A		N/A		N/A		N/A		R55
LIMITE DE MADUREZ OPTIMIZADO	660	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	1660	MENOR

De acuerdo al análisis de brecha se priorizan para este año las actividades faltantes para alcanzar el nivel 2.

5.1 Análisis de brecha Transición de IPv4 a IPv6.

Se debe realizar a fin del año 2018, con el plan de transición de IPv4 a IPv6.

5.1 Gestión de Información

U	C	S	U	U	O	Z	USUARIOS
---	---	---	---	---	---	---	----------

**MSPI Y PESI
2018-2021**

	Ciudadanía-MADS-Gobierno Nacional	Entidades Públicas Privadas - Persona Natural -Comunidades Étnicas - Asociaciones de Usuarios - Comunidad en general - Entes territoriales - Rama judicial - Entes de Control - Cooperación Internacional - Gremios.			
PRESENTACIÓN	ACCESO A LA INFORMACIÓN				
	Consulta en Línea trámites en CITA y PQRDS- PÁGINA WEB - Boletines y Comunicados - Reportes - Estadísticas - Datos Abiertos - Espacio Vital				
Y DATA ALMACENAMIENTO	Bodegas de Datos Agrupados				
	Directorio Activo - TERANAS - Servidores dedicados				
CONTINUIDAD DEL NEGOCIO	CALIDAD DE DATOS				
	Parámetros Geodatabases	Módulo de Metadatos - Geográficos - Documental - Alfanuméricos	Datos Maestros -información de usuarios	Estándares	
TELECOMUNI CACIONES	EXTRACCIÓN, TRANSFORMACIÓN Y CARGA DE BASES DE DATOS				
	Gestión de Calidad de Datos Formato, completitud, codificación estandarizada				
COMUNICACIÓN Y OPERACIONES	SERVICIOS DE INTEROPERABILIDAD (GEL-XML (MIN TIC) / OGC-ICDE))				
	Servicios Intercambio de Negocio ←	→ Catálogo de Servicios ←		→ ESB - Bus de servicios de Conectividad y Orquestaciones Complejas	
PROCESO	CERTIFICACIÓN DE OPERACIONES ESTADÍSTICAS Y/O REGISTROS ADMINISTRATIVOS				
	Lenguaje Común de Intercambio - Mapas de Intercambio -- Calidad de Datos -- Estandarización con modelos de dominios sectoriales - Directorio de Componentes -- Expediente Electrónico				
Y FÍSICA AMBIENTAL	EXTRACCIÓN TRANSFORMACIÓN Y CARGA				
	MADS	ASOCARS	ANLA	DANE	
APLICACIONES	SISTEMAS DE INFORMACIÓN				
	CITA - SISF - SINAP - INTRANET - GEOVISOR - SISTEMA DE INFORMACIÓN GEOGRÁFICO				
POLÍTICA	GOBIERNO DIGITAL	MARCO DE REFERENCIA DE ARQUITECTURA DE TI	MODELO DE GESTIÓN IT4+	SEGURIDAD DE LA INFORMACIÓN	INTEROPERABILIDAD

6 ANÁLISIS DE RIESGO PARA LA SEGURIDAD DE LA INFORMACIÓN

Acordes con la información contenida en la "Guía No. 7: Guía de gestión de riesgos"⁵ y la "Guía para la Administración del Riesgo" del DAFP⁶ se realizó el análisis de riesgo para la seguridad de la información en la Corporación.

A continuación se resumen las conclusiones del mismo:

Se identificaron 5 factores de riesgo, 3 catalogados como extremos y 2 como altos. Luego de analizadas los controles establecidos se recategorizaron estos riesgos en 1 factor de riesgo alto, 1 factor de riesgo moderado y 3 factores bajos.

Para tener el riesgo bajo control se definieron 9 acciones, las cuales tienen asociado un indicador que permite realizar el seguimiento.

7 PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

A continuación se relacionan los procedimientos que se encuentran en el Sistema de Gestión Corporativo relacionado con los procedimientos requeridos en la "Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información."⁷

7.1 Seguridad Del Recurso Humano:

Se encuentra definido en los procedimientos: "P-TH-01 VINCULACIÓN SERVIDORES PUBLICOS" Y "P-TH-08 RETIRO"

7.2 Gestión De Activos:

Se encuentra definido en los procedimientos: "D-RI-02 PRACTICAS DE ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN", "P-RI-01 COMPRAS E INFRAESTRUCTURA" y "P-RI-03 ACTIVIDADES AREA SISTEMAS"

⁵ Guía No. 7: Guía de gestión de riesgos. MINTIC 2016.

⁶ Guía para la Administración del Riesgo. DAFP 2017.

⁷ Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información. MINTIC 2016.

7.3 Control De Acceso:

Se encuentra definido en los procedimientos: "D-RI-02 PRACTICAS DE ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN" y "P-RI-03 ACTIVIDADES AREA SISTEMAS"

7.4 Criptografía: N/A

Ya que la información que se maneja en la Corporación no se requiere la encriptación de esta.

7.5 Seguridad Física Y Del Entorno:

Se encuentra definido en los procedimientos: "D-RI-02 PRACTICAS DE ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN", "P-RI-03 ACTIVIDADES AREA SISTEMAS" y las actividades del contrato de seguridad.

7.6 Seguridad De Las Operaciones:

Se encuentra definido en los procedimientos: "D-RI-02 PRACTICAS DE ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN" y "P-RI-03 ACTIVIDADES AREA SISTEMAS"

7.7 Seguridad De Las Comunicaciones:

Se encuentra definido en los procedimientos: "D-RI-02 PRACTICAS DE ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN" y "P-RI-03 ACTIVIDADES AREA SISTEMAS"

7.8 Relaciones Con Los Proveedores:

Se encuentra definido en los procedimientos: "M-RI-02 MANUAL DE CONTRATACIÓN" y "P-RI-04 CONTRATACION"

7.9 Adquisición, Desarrollo Y Mantenimiento De Sistemas De Información:

Se encuentra definido en el PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN - PETI.

7.10 Gestión De Incidentes De Seguridad De La Información:

MSPI Y PESI 2018-2021

Se tiene programado elaborarlo en 2018 con base en la "Guía para la preparación de las TIC para la continuidad del negocio" del MINTIC, 2010.

7.11 Aspectos De Seguridad De La Información De La Gestión De Continuidad De Negocio:

Se tiene programado elaborarlo en 2018 con base en la "Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información" del MINTIC, 2016.

7.12 Plan de sensibilización y apropiación del MSPI para toda la entidad.

En el "P-TH-03 FORMACIÓN, CAPACITACIÓN Y BIENESTAR" se programarán las actividades relacionadas con la seguridad de la información.

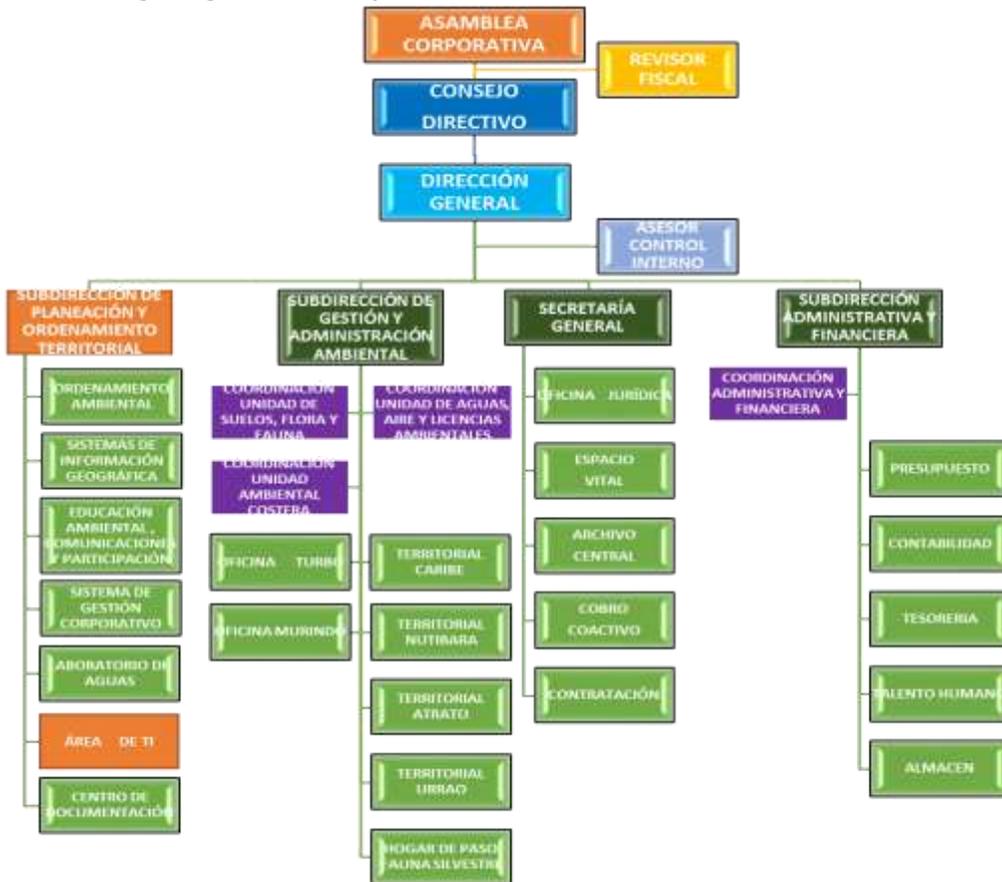
8 ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

8.1 Gobierno de SI

Basados en la "Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información" desarrollado por MINTIC y el organigrama de la Corporación se define el siguiente de SI.

**MSPI Y PESI
2018-2021**

Organigrama Corporativo



8.3 Equipo del Proyecto:

En la corporación se ha tercerizado la prestación de los servicios de TI, tales como soporte técnico, página web, Aplicativos como CITA y SINAP, etc. Cada contrato tiene definido un coordinador y un supervisor, los cuales conforman el equipo para el desarrollo del proyecto al cual deben pertenecer miembros directivos y representantes de las áreas misionales, con el propósito de asegurar que toda la información más relevante de la entidad esté disponible oportunamente. De esta forma se busca asegurar que sea una iniciativa de carácter transversal a la entidad, y que no dependa exclusivamente de la oficina o área de TI.

Una de las tareas principales del líder del proyecto es entregar y dar a conocer los perfiles y responsabilidades de cada personaje al grupo de trabajo e identificar las personas idóneas para tomar cada rol.

A continuación se presenta un modelo (adoptado de la "Guía No 4...") de los miembros del equipo de seguridad y privacidad de la información. Las funciones del comité de seguridad las asume el Comité Interinstitucional de Desarrollo Administrativo.



9 SEGUIMIENTO Y REVISIÓN DEL MSPI

- Procedimientos de seguimiento, revisión y otros controles

Ver "D-RI-02: PRACTICAS DE ADMINISTRACIÓN Y SEGURIDAD INFORMÁTICA – PROTOCOLO PARA SEGURIDAD"
- Empezar revisiones regulares de la eficacia del MSPI

Ver "D-RI-02: PRACTICAS DE ADMINISTRACIÓN Y SEGURIDAD INFORMÁTICA – PROTOCOLO PARA SEGURIDAD"
- Realizar auditorías internas del MSPI

Ver "P-MJ-09: AUDITORIAS INTERNAS"
- Empezar una revisión del MSPI, realizada por la dirección

Ver "P-DI-02: REVISIÓN POR LA DIRECCIÓN"
- Actualizar los planes de seguridad

Ver "P-DI-03 MODELO INTEGRADO DE PLANEACION Y GESTIÓN"
- Registrar acciones y eventos que podrían tener impacto en la eficacia o el desempeño del MSPI.

Ver "P-MJ-11 ADMINISTRACIÓN DEL RIESGO"
- Revisar las valoraciones de los riesgos a intervalos planificados,

Ver "P-MJ-11 ADMINISTRACIÓN DEL RIESGO"
- Medir la eficacia de los controles

Ver indicadores del SGC.
- Implementar las mejoras identificadas en el MSPI

Ver "P-MJ-08 ACCIONES PARA EL MEJORAMIENTO"

**MSPI Y PESI
2018-2021**

- Empezar las acciones correctivas y preventivas adecuadas,
Ver "P-MJ-08 ACCIONES PARA EL MEJORAMIENTO"
- Comunicar las acciones y mejoras a todas las partes interesadas,
Ver "P-MJ-08 ACCIONES PARA EL MEJORAMIENTO"
- Asegurar que las mejoras logran los objetivos previstos.
Ver "P-MJ-08 ACCIONES PARA EL MEJORAMIENTO"
- Los registros exigidos por la norma ISO 27001 y el MSPI, ej. Un libro de visitantes, informes de auditoría y formatos de autorización de acceso diligenciados.

Se programarán para el primer semestre de 2018.

Adicionalmente se ejecutar procedimientos de seguimiento, revisión y otros controles para;

- Detectar rápidamente errores en los resultados del procesamiento
- Identificar con prontitud los incidentes e intentos de violación a la seguridad, tanto los que tuvieron éxito como los que fracasaron.
- Posibilitar que la dirección determine si las actividades de seguridad delegadas a las personas o implementadas mediante tecnología de la información se están ejecutando en la forma esperada.
- Ayudar a detectar eventos de seguridad, y de esta manera impedir incidentes de seguridad mediante el uso de indicadores.
- Determinar si las acciones tomadas para solucionar un problema de violación a la seguridad fueron eficaces.

10 PLANIFICACIÓN DE ACTIVIDADES DEL MSPI

De acuerdo a los objetivos del MSPI se tienen las siguientes actividades:

Componente	Actividades	Año1	Año2	Año3	Año4
1. FASE DE PLANIFICACIÓN	1.1 Revisión de Políticas de Seguridad y Privacidad de la Información	Actualizar , aprobar y divulgar Políticas	Actualizar , aprobar y divulgar Políticas	Actualizar , aprobar y divulgar Políticas	Actualizar , aprobar y divulgar Políticas
	1.2. Revisión de Procedimientos de Seguridad de la Información.	Actualizar Procedimientos	Actualizar Procedimientos	Actualizar Procedimientos	Actualizar Procedimientos
	1.3. Roles y Responsabilidades de Seguridad	Definir y aprobar Roles y responsabilidades	Actualizar Roles y responsabilidades	Actualizar Roles y responsabilidades	Actualizar Roles y responsabilidades
	1.4. Identificación, documentación y aprobación de activos de información.	Identificar activos de información	Documentar y aprobar activos de información	Actualizar activos de información	Actualizar activos de información
	1.5. Identificación, Valoración Y Tratamiento de Riesgos.	Actualizar Riesgos	Actualizar Riesgos y realizar seguimientos	Actualizar Riesgos y realizar seguimientos	Actualizar Riesgos y realizar seguimientos
	1.6. Capacitación y sensibilización	Diseñar y aprobar programas y planes para los funcionarios sobre conciencia y comunicación de las políticas	Funcionarios toman conciencia de la seguridad y privacidad de la información.	Ejecutar planes de toma de conciencia, comunicación y divulgación.	Ejecutar planes de toma de conciencia, comunicación y divulgación.
	1.7. Implementar el Modelo de Seguridad y Privacidad de la Información	Alcanzar Madurez Inicial	Alcanzar Madurez Gestionado	Alcanzar Madurez Definido	Alcanzar Madurez gestionado cuantitativamente

**MSPI Y PESI
2018-2021**

Componente	Actividades	Año1	Año2	Año3	Año4
2. FASE DE IMPLEMENTACIÓN	2.1. Planificación y Control Operacional	Definir documentación para el control operacional	Aprobar la documentación	Ajustar de la documentación	Ajustar de la documentación
	2.2. Implementación del plan de tratamiento de riesgos	Verificar inicialmente ejecución de acciones para el tto de riesgos	Verificar ejecución de acciones para el tto de riesgos	Verificar ejecución de acciones para el tto de riesgos	Verificar ejecución de acciones para el tto de riesgos
	2.3. Indicadores De Gestión	Elaborar indicadores de gestión	Realizar seguimiento y actualizar indicadores de gestión	Realizar seguimiento y actualizar indicadores de gestión	Realizar seguimiento y actualizar indicadores de gestión
	2.4. Plan de Transición de IPv4 a IPv6	Elaborar plan de transición	Implementar plan de transición	Implementar y realizar seguimiento plan de transición	Implementar y realizar seguimiento plan de transición
3. FASE DE EVALUACIÓN DE DESEMPEÑO	3.1. Plan de revisión y seguimiento a la implementación del MSPI	Revisar el MSPI	Revisar y realizar seguimiento a mejoras del MSPI	Revisar y realizar seguimiento a mejoras del MSPI	Revisar y realizar seguimiento a mejoras del MSPI
	3.2. Plan de Ejecución de Auditorías	Planear y ejecutar auditorías	Planear y ejecutar auditorías	Planear y ejecutar auditorías	Planear y ejecutar auditorías
4. FASE DE MEJORA CONTINUA	4.1. Plan de mejora continua	Documentar el plan de mejoramiento.	Documentar el plan de mejoramiento.	Documentar el plan de mejoramiento.	Documentar el plan de mejoramiento.
	4.2. Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI	N/A	Documentar el seguimiento al plan de mejoramiento.	Documentar el seguimiento al plan de mejoramiento.	Documentar el seguimiento al plan de mejoramiento.
	4.3 Resultados del plan de ejecución de	Socializar resultados del plan	Socializar resultados del plan	Socializar resultados del plan	Socializar resultados del plan

**MSPI Y PESI
2018-2021**

Componente	Actividades	Año1	Año2	Año3	Año4
	auditorías y revisiones independientes al MSPI.				
5. MODELO DE MADUREZ	5.1. Autodiagnóstico nivel de madurez	Realizar Autodiagnóstico	Realizar Autodiagnóstico	Realizar Autodiagnóstico	Realizar Autodiagnóstico
	5.2. Identificación del nivel madurez	Realizar Autodiagnóstico	Realizar Autodiagnóstico	Realizar Autodiagnóstico	Realizar Autodiagnóstico
	5.3. Análisis de brecha	Realizar Análisis	Realizar Análisis	Realizar Análisis	Realizar Análisis
6. PRIVACIDAD DE LA INFORMACIÓN	6.1. Contar con una herramienta de análisis sobre impacto en la privacidad	N/A	Realizar la herramienta de análisis sobre impacto en la privacidad	Ajustar la herramienta	Ajustar la herramienta
	6.2. Descripción de los flujos de información	N/A	Documentar procesos	Revisar procesos documentados	Revisar procesos documentados
	6.3. Identificar los riesgos de privacidad	N/A	Elaborar matriz de riesgos de privacidad	Actualizar matriz de riesgos de privacidad	Actualizar matriz de riesgos de privacidad
7. ADOPCIÓN DEL PROTOCOLO IPV6	7.1. Plan y estrategia de transición de IPv4 a IPv6.	Elaborar el plan	Verificar y actualizar el plan	Verificar y actualizar el plan	Verificar y actualizar el plan
	7.2. Implementación del plan y estrategia de transición de IPv4 a IPv6.	N/A	Implementar el plan	Implementar el plan	Implementar el plan
	7.3. Plan de pruebas de funcionalidad de IPv4 a IPv6.	N/A	Realizar pruebas	Realizar pruebas	Realizar pruebas

**MSPI Y PESI
2018-2021**

Con base en estas actividades se elaborarán los indicadores y un tablero de control para el seguimiento de estos indicadores.

10.1 Proyección de presupuesto área de SI

Presupuesto por líneas de acción

Componente	Actividades	Recurso Humano	Recurso económico o tecnológico
1. FASE DE PLANIFICACIÓN	1.1 Revisión de Políticas de Seguridad y Privacidad de la Información	X	
	1.2. Revisión Procedimientos de Seguridad de la Información.	X	
	1.3. Roles y Responsabilidades de Seguridad	X	X
	1.4. Identificación, documentación y aprobación de activos de información.	X	
	1.5. Identificación, Valoración Y Tratamiento de Riesgos.	X	
	1.6. Capacitación y sensibilización	X	X
	1.7. Implementar el Modelo de Seguridad y Privacidad de la Información	X	X
2. FASE DE IMPLEMENTACIÓN	2.1. Planificación y Control Operacional	X	
	2.2. Implementación del plan de tratamiento de riesgos	X	X
	2.3. Indicadores De Gestión	X	

**MSPI Y PESI
2018-2021**

Componente	Actividades	Recurso Humano	Recurso económico o tecnológico
	2.4. Plan de Transición de IPv4 a IPv6	X	
3. FASE DE EVALUACIÓN DE DESEMPEÑO	3.1. Plan de revisión y seguimiento a la implementación del MSPI	X	X
	3.2. Plan de Ejecución de Auditorías	X	
4. FASE DE MEJORA CONTINUA	4.1. Plan de mejora continua	X	X
	4.2. Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI	X	
	4.3 Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.	X	
5. MODELO DE MADUREZ	5.1. Autodiagnóstico nivel de madurez	X	
	5.2. Identificación del nivel madurez	X	
	5.3. Análisis de brecha	X	
6. PRIVACIDAD DE LA INFORMACIÓN	6.1. Contar con una herramienta de análisis sobre impacto en la privacidad	X	X
	6.2. Descripción de los flujos de información	X	
	6.3. Identificar los riesgos de privacidad	X	
7. ADOPCIÓN DEL PROTOCOLO IPv6	7.1. Plan y estrategia de transición de IPv4 a IPv6.	X	X
	7.2. Implementación del plan y estrategia de transición de IPv4 a IPv6.	X	X
	7.3. Plan de pruebas de funcionalidad de IPv4 a IPv6.	X	X

11. Plan de Comunicaciones del PESI

Para alcanzar el logro de los objetivos de este plan, las actividades se encaminan a lograr una nivelación de funcionarios y usuarios por medio de tres ejes fundamentales:

- Formación.
- Acceso a la tecnología.
- Procesos institucionales acordes.

Para lograr este punto, se consideraron las siguientes acciones:

Incluir en el plan de capacitación programas de capacitación, entrenamiento y sensibilización a la incorporación de Sistemas de Información, en temas relacionados con:

- Administración De Contraseñas
- Uso Y Manejo De Inventario
- Malware y sus diferentes tipos
- Software Permitido/Prohibido En La Entidad
- Políticas Organizacionales Relacionadas Con Seguridad De La Información
- Uso De Dispositivos De La Entidad Fuera De Las Instalaciones
- Uso De Correo Electrónico E Identificación De Correos Sospechosos
- Seguridad En El Puesto De Trabajo
- Uso Apropiado De Internet
- Temas de control de acceso a los sistemas (privilegios, separación de roles)
- Política De Escritorio Limpio
- Ingeniería Social
- Sanciones Por Incumplimiento De Las Políticas
- Gestión De Incidentes (Como reportar, que puedo reportar)
- Spam
- "Shoulder Surfing" Backups Y Recuperación
- Cambios En Los Sistemas
- Amenazas Y Vulnerabilidades Comunes
- Roles Y Responsabilidades En La Entidad

11.1. Alcance

La oferta de productos definida en este ítem corresponde a una serie de productos relacionados con la preparación de las personas que se

encuentran relacionadas de manera directa e indirecta con el soporte que debe darse a funcionarios, decisores y usuarios en materia de SI.

11.2. Red de formadores de formadores

Con el fin de disminuir esfuerzos – y costos – se propone construir una red de formadores de formadores que permitan el establecimiento y difusión de los siguientes temas:

- Redes de conocimiento.
- Círculos de conocimiento.
- Gestión del conocimiento.
- Pedagogía para no pedagogos.
- Modelos educativos.
- Diseño de contenidos para entornos virtuales.