Tabla de contenido

1. OBJETIVOS

1.1. OBJETIVOS GENERAL

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de Empocaldas S.A. E.S.P., para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la gestión de implementación de las estrategias de seguridad definidas.

1.2 . OBJETIVOS ESPECÍFICOS

- Definir y establecer la estrategia de seguridad digital.
- Definir y establecer las necesidades de Empocaldas S.A. E.S.P. para la implementación del Sistema de Gestión de Seguridad de la Información.
- Priorizar los proyectos a implementar para la correcta implementación del SGSI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.

2. ALCANCE

El Plan Estratégico de Seguridad de la Información al buscar la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de Empocaldas S.A. E.S.P., comparte el alcance definido dentro de la Política General de Seguridad de la Información, donde se indica que La implementación del Modelo de Seguridad y Privacidad de la Información conforme a los requisitos normativos comprende a todos los procesos de la entidad.

3. DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- 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*", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.

- Resolución 500 de 2021. "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*".
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- Decreto 338 de 2022 por medio del cual se 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.
- Directiva presidencial 003 de 2021, lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado 'de la protección de la información y de los datos'- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1712 de 2014, Por medio del cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional."
- Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital
- Resolución 746 de 2022, por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021.
- 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.
- Anexo 4, lineamientos para la gestión de riesgos de seguridad digital en entidades públicas.
- Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - diciembre de 2020

4. ESTADO DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Tomando como insumo la medición del FURAG 2021 para Empocaldas S.A. E.S.P. en temas de Seguridad de la información el estado actual de la entidad respecto fortalecimiento de la Seguridad y Privacidad de la Información se encuentra con un puntaje de referencia de 92,3 de 96,1 que sería el puntaje máximo de referencia a obtener en el habilitador de Seguridad y Privacidad de la Información.

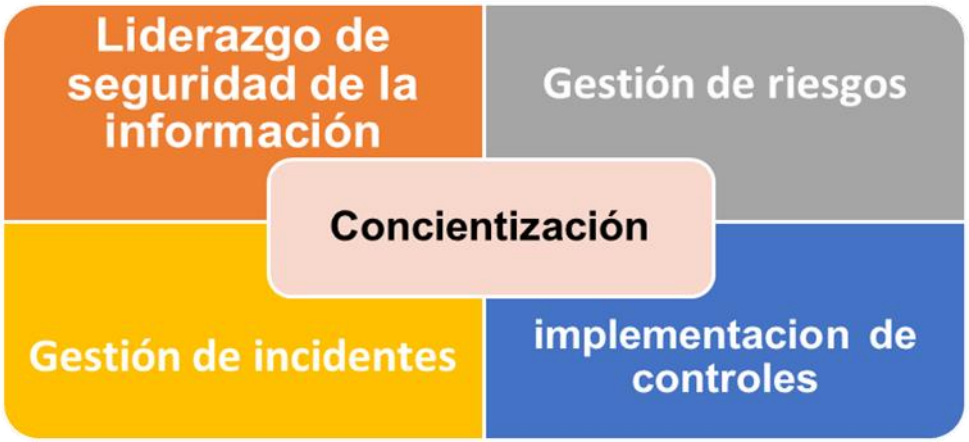
Las recomendaciones para continuar con el avance y el mejoramiento continuo para dicho habilitador son:

- 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, aprobarlo mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua.
- Definir indicadores para medir la eficiencia y eficacia del sistema de gestión de seguridad y privacidad de la información (MSPI) de la entidad, aprobarlos mediante el comité de gestión y desempeño institucional, implementarlos y actualizarlos mediante un proceso de mejora continua.

5. ESTRATEGIA DE SEGURIDAD DIGITAL

Empocaldas S.A. E.S.P. establece una estrategia de seguridad digital en la que se integra los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes de seguridad digital, así mismo, establecer los lineamientos y estándares para la estrategia de seguridad digital.

Por tal motivo, *Empocaldas S.A. E.S.P.* define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



5.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

Objetivos	
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los jefes de las diferentes áreas y secciones de la Entidad.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

5.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, Empocaldas S.A. E.S.P. define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

ESTRATEGIAS	PROYECTO	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	Desarrollar e implementar una política de seguridad Mejorar la coordinación entre el departamento de RRHH y el departamento TIC	Política General de seguridad de la información. Manual de Políticas de Seguridad de la Información
Gestión de riesgos	Proyecto 1: Identificar, valorar y clasificar los riesgos asociados a los activos de información Proyecto 2: Definir planes de tratamiento de riesgos de seguridad Proyecto 3: Realizar una gestión efectiva de la seguridad de la información y la seguridad digital en la entidad. Proyecto 4: Reportar los resultados del análisis de riesgos y gestión de incidentes al comité institucional de gestión y desempeño o quien haga sus veces Proyecto 5: Establecer necesidades de capacitación que deben recibir los funcionarios de la entidad en temas relacionados con seguridad digital y las nuevas amenazas cibernéticas. Proyecto 6: Determinar los recursos técnicos, humanos y administrativos de seguridad de la información y seguridad digital, necesarios para la entidad. Proyecto 7: Implementar y gestionar un Sistema de Gestión de Seguridad de la Información de acuerdo con lo establecido en el Modelo de Seguridad y Privacidad de la Información, que permita gestionar los riesgos de seguridad de la información de la entidad de una manera adecuada y oportuna. Proyecto 8: Cumplir los lineamientos de gestión del riesgo establecidos en la guía para la administración del riesgo y el diseño de controles en entidades públicas	Matriz de riesgos de seguridad digital. Definir planes de tratamiento de riesgos. Capacitaciones integradas en el Plan Anual de Capacitaciones. Plan de Seguridad y Privacidad de la Información. Modelo se Seguridad y Privacidad de la Información.

ESTRATEGIAS	PROYECTO	PRODUCTOS ESPERADOS
	expedida en el marco del modelo integrado de planeación y gestión.	
Concientización	Proyecto 1: Realizar jornadas de sensibilización a todo el personal. Proyecto 2: Realizar trasferencia de conocimiento a colaboradores de la Entidad a través de cursos especializados en diferentes temas. Proyecto 2: Medir el grado de sensibilización a toda la Entidad. Proyecto 3: Realizar jornadas de sensibilización a todo el personal. Proyecto 4: Realizar trasferencia de conocimiento a colaboradores de la Entidad a través de cursos especializados en diferentes temas. Proyecto 5: Medir el grado de sensibilización a toda la Entidad.	Evidencias de las actividades desarrolladas Certificaciones de cursos Resultado de las encuestas de medición
Implementación de controles	Control 1: Procedimiento de copias de seguridad. Control 2: Identificación y clasificación de la información. Control 3: Definición y asignación de roles y responsabilidades de la seguridad de la información. Control 4: Exigencia de la dirección a todos los empleados y contratistas de la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización. Control 4: Implementación de proceso formal de registro y cancelación de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios.	Procedimiento de copias de seguridad. Inventario de activos de información. Definición de roles y responsabilidades Comunicado exigencia aplicación y cumplimiento de las políticas de seguridad y privacidad de la información. Proceso de registro y cancelación de usuarios.
Gestión de incidentes	Proyecto 1: Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información. Proyecto 2: Capacitar al personal en la gestión de incidentes de seguridad de la información.	Procedimiento de Gestión de Incidentes de Seguridad.

ESTRATEGIAS	PROYECTO	PRODUCTOS ESPERADOS
	Proyecto 3: Designar dentro de la entidad los responsables de gestionar y dar respuesta a los incidentes de seguridad digital, liderado por el responsable de seguridad digital. Proyecto 4: En el momento de identificar un incidente de seguridad digital catalogado como muy grave o grave, dar reporte ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital).	Sesiones de capacitación desarrolladas. Roles y responsables de la gestión y tratamiento de riesgos de seguridad digital. Formato reporte de incidentes de seguridad establecido por el CSIRT debidamente diligenciado.

5.3 CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

ACTIVIDAD	Fecha Iniciación	Fecha Terminación	Responsable
ADQUISICIÓN DE CINTAS PARA BACKUPS CUSTODIA DE INFORMACIÓN, ADQUISICIÓN ELEMENTOS, ACCESORIOS Y KIT DE MANTENIMIENTO EQUIPOS SECCIONAL MANIZALES Y ACCESORIOS PARTES PARA LA PLATAFORMA TECNOLÓGICA, ELEMENTOS PARA REPOTENCIAR EQUIPOS	1/05/2023	30/12/2023	Sección Sistemas
GESTIONAR EL MANTENIMIENTO PREVENTIVO Y CORRECTIVO UPS MANIZALES - DORADA - CHINCHINÁ - CAMBIO BATERÍAS UPS MANIZALES - ADQUISICION BATERIAS	1/04/2023	31/12/2023	Sección Sistemas
CONTRATAR LA PRESTACION SERVICIOS PARA LA REALZACION DE DOS (2) MANTENIMIENTOS PREVENTIVOS(5) AIRES ACONDICIONADOS DORADA Y ADQUISICIÓN 2 AIRES ACONDICIONADOS Y SENSOR DE HUMEDAD PARA LA SECCIONAL MANIZALES	1/04/2023	31/12/2023	Sección Sistemas
GESTIONAR LA RENOVACIÓN DE EXTENSIÓN DE GARANTÍAS PARA LOS EQUIPOS SERVIDORES DEL DATA CENTER.	1/07/2023	31/10/2023	Sección Sistemas
GESTIONAR LA RENOVACIÓN LICENCIAMIENTO SUSCRIPCIÓN ANUAL FIREWALL - RENOVACIÓN FORTICLIENTE ENDPOINT - ADQUISICIÓN DNSSEC - RENOVACIÓN POOL DE LICENCIAS IPV6	1/02/2023	31/05/2023	Sección Sistemas
GESTIONAR LA RENOVACIÓN LICENCIAMIENTO VEEAM BACKUP PARA OFFICE 365 POR SUSCRIPCIÓN A UN AÑO.	1/03/2023	31/05/20223	Sección Sistemas

5.4 ANÁLISIS PRESUPUESTAL:

NOMBRE DEL PROYECTO	AÑO 2023												COSTO PROYECTO
	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	
ADQUISICIÓN DE CINTAS PARA BACKUPS CUSTODIA DE INFORMACIÓN, ADQUISICIÓN ELEMENTOS, ACCESORIOS Y KIT DE MANTENIMIENTO EQUIPOS SECCIONAL MANIZALES Y ACCESORIOS PARTES PARA LA PLATAFORMA TECNOLÓGICA, ELEMENTOS PARA REPOTENCIAR EQUIPOS													$ 39.000.000
GESTIONAR EL MANTENIMIENTO PREVENTIVO Y CORRECTIVO UPS MANIZALES - DORADA - CHINCHINÁ - CAMBIO BATERÍAS UPS MANIZALES - ADQUISICION BATERIAS													$ 8.000.000
CONTRATAR LA PRESTACION SERVICIOS PARA LA REALZACION DE DOS (2) MANTENIMIENTOS PREVENTIVOS(5) AIRES ACONDICIONADOS DORADA Y ADQUISICIÓN 2 AIRES ACONDICIONADOS Y SENSOR DE HUMEDAD PARA LA SECCIONAL MANIZALES													$ 23.000.000
GESTIONAR LA RENOVACIÓN DE EXTENSIÓN DE GARANTÍAS PARA LOS EQUIPOS SERVIDORES DEL DATA CENTER.													$ 16.000.000
GESTIONAR LA RENOVACIÓN LICENCIAMIENTO SUSCRIPCIÓN ANUAL FIREWALL - RENOVACIÓN FORTICLIENTE ENDPOINT - ADQUISICIÓN DNSSEC - RENOVACIÓN POOL DE LICENCIAS IPV6													$ 45.000.000
GESTIONAR LA RENOVACIÓN LICENCIAMIENTO VEEAM BACKUP PARA OFFICE 365 POR SUSCRIPCIÓN A UN AÑO.													$ 21.000.000

6. RESPONSABLES

Alta Gerencia: Velar por la implementación del MSPI y garantizar los recursos requeridos.
Comité Institucional de Gestión y Desempeño: Aprobar los documentos de Alto Nivel.
Grupo de Tecnología: Coordinar las actividades de implementación del MSPI
Control Interno

7. APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección y el comité de gestión y desempeño institucional con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

Elaboró o Actualizó	Revisó y Aprobó
Jefe Sección Sistemas	(Acta 2 - 2023-01-25) COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO