PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DEL DEPARTAMENTO DEL CESAR

Valledupar, Noviembre de 2019

TABLA DE CONTENIDO

INTRODUCCIÓN

El Departamento del Cesar, en cumplimiento a las Políticas y Directrices establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones, el Decreto 612 del 4 de Abril de 2018, Decreto 1078 de 2015 y la NTC/IEC ISO 27001:2013, implementará actividades de planeación estratégica para el control y administración efectiva de los riesgos y las necesidades de seguridad de la información de la entidad.

Una vez socializado el presente plan, los funcionarios, contratistas y terceros de la entidad adoptarán los controles de seguridad y privacidad de la información en sus procesos, con el fin de minimizar los riesgos que puedan afectar la seguridad y privacidad de la información.

1. OBJETIVO GENERAL

Establecer el plan de implementación y seguimiento del Modelo de seguridad y privacidad de la información del Departamento del Cesar.

1.1. OBJETIVOS ESPECÍFICOS

- Determinar las actividades de la fase del diagnóstico de la entidad previo a la implementación del Modelo de Seguridad y Privacidad de la información.
- Describir las actividades de la fase de planeación del Modelo de Seguridad y Privacidad de la entidad.
- Identificar las actividades de la fase de implementación del Modelo de Seguridad y Privacidad de la entidad.
- Establecer las actividades de la fase de evaluación del desempeño del Modelo de Seguridad y Privacidad de la entidad.
- Describir las actividades de la fase de mejora continua del Modelo de Seguridad y Privacidad de la entidad.

2. ALCANCE

Aplica a todos los Procesos, a todos sus funcionarios, contratistas y terceros que en razón del cumplimiento de sus funciones y las del Departamento compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación. Así mismo, esta Plan aplica a toda la información creada, procesada o utilizada por la entidad, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

3. MARCO NORMATIVO

3.1. DECRETOS Y LEYES QUE APLICAN

- **LEY 527/99:** Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.
- **LEY 594/00:** Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.
- **CONPES 3701 DE 2011:** Lineamientos de política para ciberseguridad y Ciberdefensa
- **LEY 1581/12:** Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.
- **LEY 1221 DE 2008:** promover y regular el teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones.
- **LEY 1712 DE 2014**. “Ley de transparencia y del derecho de acceso a la Información pública nacional”.
- **LA LEY 1581** de 2012 y decreto 1377 de 2013. “Ley de protección de datos personales”.
- **LEY 1273 DE 2009**. “Ley de delitos informáticos y la protección de la información y de los datos”.
- **DECRETO 1078** del 26 de mayo de 2015. Por medio del cual se expide el “Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.
- **LEY 527/1999.** “Acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.
- **DECRETO 612** del 4 de abril de 2018, "por el cual se fijan directrices para la integración de planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado".
- **DECRETO 1008 DEL 14 DE JUNIO DE 2018**, "Por el cual se establecen los lineamientos generales de la política Gobierno Digital

- **DECRETO 884 DE 2012:** Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.

3.2. BASES METODOLÓGICAS

- Norma ISO/IEC 27001:2013.
- Modelo de Seguridad y Privacidad de la Información de Gobierno Digital –MSPI
- Instrumento de Evaluación MSPI MINTIC

4. DEFINICIONES

ACTIVO: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

ALCANCE: ámbito de la organización que queda sometido al SGSI.

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

ANÁLISIS DE RIESGOS: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

ANÁLISIS DE RIESGOS CUALITATIVO: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

ANÁLISIS DE RIESGOS CUANTITATIVO: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

CONTROL: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

CONTROL CORRECTIVO: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

CONTROL DETECTIVO: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

CONTROL DISUASORIO: Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.

CONTROL PREVENTIVO: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

ESTIMACIÓN DE RIESGOS: Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

EVALUACIÓN DE RIESGOS: Proceso global de identificación, análisis y estimación de riesgos.

FASE DIAGNOSTICO: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

FASE EVALUACIÓN DE DESEMPEÑO (VERIFICAR**):** Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.

FASE IMPLEMENTACIÓN (HACER): En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.

FASE PLANIFICACIÓN (PLANEAR**):** En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.

FASE MEJORA CONTINUA (ACTUAR**):** Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

GESTIÓN DE RIESGOS: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

INVENTARIO DE ACTIVOS: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud.

ISO/IEC 27001:2013: Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI): El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

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.

RIESGO RESIDUAL: El riesgo que permanece tras el tratamiento del riesgo.

SELECCIÓN DE CONTROLES: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

5. FASE DE DIAGNÓSTICO – ETAPAS PREVIAS A LA IMPLEMENTACIÓN

ACTIVIDADES	RESPONSABLES	REGISTROS	CRONOGRAMA		REALIZADO
			FECHA INICIO	FECHA FINAL	
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Herramienta de Diagnóstico MSPI - MINTIC	01/01/2018	28/02/2018	100%
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Herramienta de Diagnóstico MSPI - MINTIC	01/03/2018	30/04/2018	100%
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Herramienta de Diagnóstico MSPI - MINTIC	01/05/2018	31/12/2018	100%
Identificar el avance de la	Profesional Especializado	Herramienta de	01/07/2018	30/07/2018	100%

implementación del ciclo de operación al interior de la entidad.	asignado al Grupo de Recursos Físicos y Tecnológicos.	Diagnóstico MSPI - MINTIC			
Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Herramienta de Diagnóstico MSPI – MINTIC Política de protección de datos personales – Decreto 00222 del 22 de Agosto de 2019	01/08/2018	30/08/2018	100%
Identificación del uso de buenas prácticas en ciberseguridad.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Herramienta de Diagnóstico MSPI - MINTIC	01/08/2018	30/08/2018	100%

6. FASE DE PLANIFICACIÓN

ACTIVIDADES	RESPONSABLES	REGISTROS	CRONOGRAMA		REALIZADO
			FECHA INICIO	FECHA FINAL	
Definir la Política de seguridad y privacidad de la información	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Documento con la política de seguridad de la información, aprobado por la alta Dirección y socializada al interior de la Entidad.	01/02/2019	31/12/2019	100%
Procedimientos de seguridad de la información.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	01/08/2019	30/04/2020	20%
Roles y responsabilidades de seguridad y privacidad de la información.	Comité Institucional de Gestión y Desempeño en la Administración Departamental.	Acto administrativo a través del cual se crea o se modifica las funciones del comité institucional de gestión y desempeño (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información	23/08/2019	30/04/2020	0%

		en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.			
Identificación del Inventario de activos de información.	Secretaría General Comité Institucional de Gestión y Desempeño en la Administración Departamental.	Matriz con la identificación valoración y clasificación de activos de información.	04/03/2019	31/12/2019	100%
Integración del MSPI con el Sistema de Gestión documental	Secretaría General	Documento de Plan de Preservación Digital	04/03/2019	31/12/2019	100%
Identificación, Valoración y tratamiento de riesgo.	Comité Institucional de Gestión y Desempeño en la Administración Departamental.	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección.	04/03/2019	30/04/2020	50%
Plan de Comunicaciones	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Documento con el plan de comunicación sensibilización y capacitación para la entidad.	04/03/2019	28/02/2020	0%
Plan de diagnóstico de IPv4 a IPv6. Resolución 00027210 de 3 octubre de 2017 del MINTIC.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Documento con el Plan de diagnóstico para la Transición de IPv4 a IPv6.	04/03/2019	30/04/2020	0%

7. FASE DE IMPLEMENTACIÓN

ACTIVIDADES	RESPONSABLES	REGISTROS	CRONOGRAMA		REALIZADO
			FECHA INICIO	FECHA FINAL	
Planificación y Control	Profesional Especializado	Documento con la	01/01/2019	30/04/2020	0%

Operacional.	asignado al Grupo de Recursos Físicos y Tecnológicos.	estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección. (Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad).			
Implementación del plan de Tratamiento de riesgos.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Documento con la declaración de aplicabilidad. Documento con el plan de tratamiento de riesgos.	01/11/2019	30/04/2020	0%
Indicadores De Gestión.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	01/06/2020	30/07/2020	0%
Plan de Transición de IPv4 a IPv6	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado la entidad	01/01/2020	31/12/2020	0%

8. FASE DE EVALUACIÓN DEL DESEMPEÑO

ACTIVIDADES	RESPONSABLES	REGISTROS	CRONOGRAMA		% DE EJECUCIÓN
			FECHA INICIO	FECHA FINAL	
Plan de revisión y Seguimiento, a la implementación del MSPI.	Profesional Especializado asignado al Grupo de Recursos Físicos y Tecnológicos.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	01/02/2020	Revisión Semestral a partir de la Fecha de Inicio	0%
Plan de Ejecución de Auditorias	Oficina de Control Interno de Gestión	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.	01/02/2020	No aplica	0%

9. FASE DE MEJORA CONTINUA

ACTIVIDADES	RESPONSABLES	REGISTROS	CRONOGRAMA		% DE EJECUCIÓN
			FECHA INICIO	FECHA FINAL	
Plan de Mejora Continua	Comité Institucional de Gestión y Desempeño en la Administración Departamental.	Documento con el plan de mejoramiento . Documento con el plan de comunicación de resultados.	01/02/2020	No aplica	0%

CONTROL DE CAMBIOS

FECHA	VERSION	CAMBIOS
18/01/2019	VER- 1.0	