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

INTRODUCCIÓN

La Gobernación del Cesar en cumplimiento a las Políticas y Directrices, establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones y en el marco de las normas Nacionales (Decreto 612 del 4 de Abril de 2018 y Decreto 1078 de 2015) e Internacionales (ISO 27001:2013), implementará los lineamientos que le permitan planear, diseñar, desarrollar y poner en marcha el PLAN DE SEGURIDAD DE LOS ACTIVOS DE INFORMACION DE LA GOBERNACION DEL CESAR adoptando el modelo PHVA (Planear-Hacer-Verificar-Actuar) aplicado al Modelo de Seguridad y Privacidad de la Información MSPI.

La Gobernación del Cesar, a través del PLAN DE SEGURIDAD DE LOS ACTIVOS DE INFORMACION, busca blindar los activos de información que hacen parte de la entidad, realizando las acciones que conduzcan y permitan identificar el riesgo, identificar sus amenazas, la probabilidad de ocurrencia y aplicar los controles de seguridad y privacidad de la información que impidan o reduzcan la materialización del riesgo.

La entidad, una vez comunicado y socializado el Modelo de seguridad y Privacidad de la información deberá solicitarles a los funcionarios, contratistas y terceros la aplicación de los controles de seguridad y privacidad de la información en cada uno de los procesos y procedimientos que se encuentren alineados a sus funciones, con el fin de desarrollar cada una de las actividades con el menor riesgo que permita afectar la seguridad, privacidad y confidencialidad de la información.

OBJETIVO GENERAL

Es documentar la planeación, diseño, implementación y seguimiento de las acciones que se realizaran en los plazos establecidos en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) de la Gobernación del Cesar

OBJETIVOS ESPECÍFICOS

Elaborar la arquitectura del plan de seguridad de los activos de información de la Gobernación del Cesar de acuerdo al modelo PHVA que se aplica al Modelo de Seguridad y Privacidad de la Información de la entidad.

- Implementar los controles de acceso a los activos de información de la Gobernación del Cesar.
- Comunicar y sensibilizar la política de Seguridad y Privacidad de la Información de la Gobernación del Cesar
- Definir el cronograma de actividades y las labores que se realizaran anualmente con el fin de alcanzar el 100% de la implementación del Modelo de Seguridad y Privacidad de la Información.
- Incentivar a los funcionarios, contratistas y terceros que realicen acciones que contribuyan a la seguridad, privacidad e Integridad de la información.
- Generar un listado de los incidentes que se presentan en materia de tecnología TI, con sus respectivas soluciones.

JUSTIFICACIÓN

La información, es uno de los activos de información más importante de una entidad, sin ella no podríamos realizar un proceso de planeación, y mucho menos tomar decisiones, establecer estrategias y alcanzar metas, por ello se hace necesario implementar un plan de seguridad de activo de información q ue busca identificar los lineamientos, directrices y acciones que se realizaran con el fin poner en marcha el Modelo de Seguridad y Privacidad de la Información (MSPI) de la entidad.

El plan de seguridad de activo de información definirá los plazos anuales, las labores a desarrollar, los controles que se implementaran, identificar la amenaza, controles existentes, todo esto con el objetivo de mitigar, minimizar, reducir, eliminar o trasladar el riesgo con el fin de conservar la privacidad, la integridad y disponibilidad de la información de la gobernación del cesar.

ALCANCE Y DELIMITACIÓN DEL PLAN

Inicia con trazar y planificar la manera como la entidad realizará o continuará con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y termina con la implementación de los controles de seguridad y privacidad de la información de tal forma que permita mitigar o reducir el riesgo, solo aplica para los activos de información de la entidad.

MARCO NORMATIVO

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.

MARCO METODOLOGICO

PLAN DE SEGURIDAD DE LA INFORMACIÓN: https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html
ARTICLES-5482_G8_CONTROLES_SEGURIDAD:
https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html
ARTICLES-5482_MODELO_DE_SEGURIDAD_PRIVACIDAD:
https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

GLOSARIO

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.

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.

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

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

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.

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.

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.

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.

METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL PLAN GENERALDE SEGURIDAD DE LA INFORMACIÓN.

La metodología implementada, para elaborar el Modelo de Seguridad y Privacidad de la información de la entidad, es el modelo P.H.V.A, siguiendo los lineamientos del Ministerio de Tecnología de Información y las comunicaciones a través de la **guía articles-5482_Modelo_de_Seguridad_Privacidad** y el Instrumento de evaluación **articles-5482_Instrumento_Evaluacion_MSPI.xls** que se encuentra en la Dirección Web https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html.

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.

A continuación se describe el ciclo de funcionamiento del modelo de operación, a través de la descripción detallada de cada una de las cinco (5) fases que lo comprenden.

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 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 Implementación (Hacer**):** En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.

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 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.

		ACTIVIDAD	2018												2019												2020											
		FASE DE DIAGNOSTICO	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12
FASE DE DIAGNÓSTICO - ETAPAS PREVIAS A LA IMPLEMENTACIÓN		Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.																																			
		Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad																																			
		Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.																																			
		Identificar el avance de la implementación del ciclo de operación al interior de la entidad.																																			
		Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.																																			
		Identificación del uso de buenas prácticas en ciberseguridad.																																			
MODELO P.H.V.A		FASE DE PLANIFICACIÓN																																			
	PLANIFICAR	Realizar análisis de Contexto de la Entidad en torno a la seguridad.																																			
		Definir la Políticas de seguridad y privacidad de la información																																			
		Procedimientos de seguridad de la información.																																			
		Definir el Alcance y Limites del MSPI																																			
		Roles y responsabilidades de seguridad y privacidad de la información.																																			
		Identificación del Inventario de activos de información.																																			
		Integración del MSPI con el Sistema de Gestión documental																																			
		Identificación, Valoración y tratamiento de riesgo.																																			
		Metodologia de valoración del riesgo																																			
		Criterios de aceptación del Riesgo, Identificar los Niveles de Riesgo Aceptable																																			
		Seleccionar los objetivos de control, y los controles para el tratamiento de Riesgo																																			
		Establecer el Plan de Capacitación, Comunicación y Sensibilización																																			
		Plan de diagnóstico de IPv4 a IPv6.																																			
	HACER	FASE IMPLEMENTACION																																			
		Implementar o Ejecutar los objetivos de control, y los controles para el tratamiento de Riesgo																																			
		Implementar o Ejecutar el plan de tratamiento de riesgos.																																			
		Implementar procedimiento de gestión de vulnerabilidades																																			
		Ejecutar pruebas anuales de vulnerabilidades																																			
		Indicadores De Gestión.																																			
		Ejecutar del plan y estrategia de transición de IPv4 a IPv6.																																			
	VERIFICAR	FASE DE EVALUACIÓN DE DESEMPEÑO																																			
		Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección																																			
		Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.																																			
	ACTUAR	FASE DE MEJORA CONTINUA																																			
		Diseñar Plan de mejora continua																																			

PLAN DE IMPLEMENTACION DEL MODELO DE SEGURIDAD

MODELO DEL NIVEL DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION - MSPI

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

ESCALA DE VALORACION DE LOS CONTROLES

Tabla de Escala de Valoración de Controles ISO 27001:2013 ANEXO A		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.

Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

CONTROL DE CAMBIOS

FECHA	VERSION	CAMBIOS
18/01/2019	VER- 1.0	