INSTITUTO DE PATRIMONIO Y CULTURA DE CARTAGENA DE INDIAS - IPCC

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÒN 2024

CARMEN LUCY ESPINOSA DIAZ

Directora

TABLA DE CONTENIDO

Contenido

INTRODUCCIÒN

Teniendo en cuenta la importancia de la información y apoyados en su significado, como el conjunto organizado de datos generados, obtenidos, transformados o controlados que constituyen un mensaje sin importar el medio en que se contenga (digital y no digital); nace la necesidad de definir normativas y buenas prácticas para su tratamiento general dentro de la entidad.

El presente documento nos describe las medidas que implementará la **Instituto de Patrimonio y Cultura de Cartagena - IPCC**, para la seguridad y privacidad de la información que se maneja en la entidad, según lo establecido en el decreto 1008 del 14 de junio de 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.

1. ALCANCE

Mediante este plan se aplicará el Modelo de Seguridad y Privacidad de la Información que enmarcará todo activo de información integrado en los procesos del **Instituto de Patrimonio y Cultura de Cartagena - IPCC**, los cuales incluyen: funcionarios, contratistas, sistemas de información, equipo de cómputo, servidores y todo lo que se incluya en el inventario de activos de información.

2. OBJETIVO

Establecer un plan que permitirá adoptar el Modelo de Seguridad y Privacidad de la información, el cual manifiesta la posición de la entidad con respecto a la importancia que tienen los activos de información para el cumplimiento de las funcionen misionales.

2.1 OBJETIVOS ESPECÍFICOS

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la entidad
- Crear las políticas y procedimientos en materia de seguridad y privacidad de la información.
- Establecer los Roles y responsabilidades de seguridad y privacidad de la información
- Generar una cultura de seguridad y privacidad de la información en los funcionarios, contratistas y ciudadanos. (plan de comunicaciones fase planificación)
- Minimizar los riesgos asociados con los activos de información.
- Garantizar la continuidad del negocio frente a incidentes.

3. VIGENCIA

El presente documento, mediante el cual el Instituto de patrimonio y cultura de Cartagena Ipcc, establece los lineamientos y/o Políticas de Seguridad, estará vigente desde el momento en que sea aprobado por la Alta Dirección.

La vigencia del presente documento estará sujeta a los cambios normados por el gobierno nacional, y si surge la necesidad de actualizar el documento conforme a las exigencias del IPCC, o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica.

Nota: El presente plan no tiene una fecha especifica de vigencia, toda vez las disposiciones y lineamientos emitidos por el MinTic señalan que las entidades deben establecer una vigencia permanente de los procesos de Seguridad y Privacidad de la Información; En caso de haber una variación específica en la vigencia, esta será modificada únicamente por los lineamientos emitidos por el Gobierno Nacional

4. PRINCIPIOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Proteger la información creada, procesada, transmitida o resguardadapor los procesos de la entidad, con el fin de minimizar impactos financieros, operativos, reputaciones o legales debido a un uso incorrecto de esta.
- Proteger la información de las amenazas originadas por parte de funcionarios o contratistas.
- Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos críticos.
- Implementará control de acceso a la información, sistemas y recursos de red.
- Propender que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- Establecer una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información para una mejora efectiva de su modelo de seguridad.
- Verificar la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- Dar cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
- Definir, implementar, operar y mejorar de forma continua un modelo de seguridad y privacidad de la información, soportado en lineamientos claros alineados a las necesidades de las partes interesadas, y a los requerimientos regulatorios que le aplican a su naturaleza.
-

5. CICLO DE OPERACIONES DEL MODELO DE SEGURIDAD DE LA INFORMACION

A continuación, se describen el ciclo de operación establecido por medio de cinco (5) fases, cada una con una serie de actividades que se ejecutarán junto con los respectivos entregables, en aras de cumplir con los objetivos propuestos:

A continuación, se describe en la tabla la actividad tomadas del modelo guía del Min TIC, así como el entregable las cuales se ejecutan en cada fase del ciclo de operaciones en seguridad de la información.

FASE	ACTIVIDADES	ENTREGABLE/RESULTADO
1. FASE DE DIAGNÓSTICO	Análisis de la normativa vigente a cumplir por del IPCC relacionada con la Privacidad y Protección de los datos personales	Normograma relacionado con Seguridad de la información, Privacidad y Protección de Datos personales
	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la entidad.	Documento del diagnóstico.
	Identificar el nivel de madurez de seguridad y privacidad de la información en la entidad	
	Identificar vulnerabilidades que sirvan como insumo para la fase deplanificación.	
2. FASE DE PLANIFICACIÓN	Identificar el alcance y objetivos de seguridad y privacidad de la información	Documento con la política de seguridad de la información.
	Establecer Política de seguridad y privacidad de la información	
	Determinar roles y responsabilidades de seguridad y privacidad de la información.	
	Políticas de seguridad y privacidad de la información	- Política General del MSPI. - Manual con las políticas y procedimientos de seguridad y privacidad de la información.
	Establecer los procedimientos de seguridad de la información.	

	Realizar el inventario de activos deinformación.	Documento con la metodología para identificación, clasificación y valoración de activos de información.
		Matriz con la identificación, valoración y clasificación de activos de información.
	Identificar y valorar el tratamiento de riesgo de la información.	Documento con el plan de tratamiento de riesgos.
		Documento con la declaración de aplicabilidad.
		Matriz de riesgos
	Realizar y ejecuta Plan de comunicaciones y divulgación del Plan	Documento con el plan de comunicación, sensibilización y capacitaciónpara la entidad.
3. FASE DE IMPLEMENTACIÓN	Construir la planificación y control operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
	Implementar el plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño decada proceso.
	Diseñar los Indicadores de gestión de seguridad y privacidad de la información	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.
	Revisar y realizar seguimiento a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado porla alta Dirección.

4. FASE DE EVALUACIÓN DE DESEMPEÑO	Atender las auditorías del plan de Seguridad y Privacidad de la Información	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.
5. FASE DE MEJORACONTINUA	Plan de mejora continua	Documento con el plan de mejoramiento.
		Documento con el plan decomunicación de resultados.

Tabla No 1. Fases y actividades en el ciclo de operación en Seguridad de la Información

6. CICLO DE OPERACIONES PARA LA PRIVACIDAD Y PROTECCIÓN DE LOS DATOS PERSONALES

El Instituto de Patrimonio y Cultura de Cartagena, con la finalidad de proveer el acceso a la información pública; así como también de garantizar los derechos de los titulares de los datos, proteger los derechos de autor y amparar los secretos profesionales, proyecta por medio del MSPI afianzar el tratamiento adecuado de los datos e información que le es entregada como custodio y responsable de salvaguardarla y garantizar la transparencia en su administración.

La privacidad y protección de los datos se deben establecer desde diferentes perspectivas y ámbitos; se debe tener presente que todo el Sistema de Información que capture datos biométricos, audio, video, fotos, datos clínicos, entre otros deben ser tratados como datos sensibles; es menester analizar e involucrar todo el proceso del Diseño y ejecución de un sistema de gestión documental, desarrollar políticas, procedimientos, mecanismos que impliquen el tratamiento de información personal

7. MADUREZ DEL MSPI

Para una adecuada gestión de la privacidad, protección y seguridad de la información se debe ir evolucionando en la madurez asociado a la evolución de su puesta en marcha y adopción del mismo en la transversalidad de las operaciones encausado a amprar la confidencialidad, integridad y disponibilidad de la información; además de contribuir a la construcción de una entidad más transparente a través del componente de gobierno Digital. Para la evaluación se tomará en relación a las características de los niveles de madurez enunciados en el Ministerio de Tecnologías de Información y las Comunicaciones – MinTIC en el documento guía MSPI

Nivel	Descripción
Inexistente	• Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros; sin embargo, no están alineados a un Modelo de Seguridad. • No se reconoce la información como un activo importante para su misión y objetivos estratégicos. • No se tiene conciencia de la importancia de la seguridad de la información en la entidad
Inicial	• Se han identificado las debilidades en la seguridad de la información. • Los incidentes de seguridad de la información se tratan de forma reactiva. • Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las

	amenazas sobre seguridad de la información que se presentan en la Entidad.
Repetible	• Se identifican en forma general los activos de información. • Se clasifican los activos de información. • Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información. • Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión. • La entidad cuenta con un plan de diagnóstico para IPv6.
Definido	• La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información. • La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información. • La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas. • La Entidad tiene procedimientos formales de seguridad de la Información • La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información. • La Entidad ha realizado un inventario de activos de información aplicando una metodología. • La Entidad trata riesgos de seguridad de la información a través de una metodología. • Se implementa el plan de tratamiento de riesgos. • La entidad cuenta con un plan de transición de IPv4 a IPv6
Administrado	• Se revisa y monitorea periódicamente los activos de información de la Entidad. Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información. • Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro. • La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.
Optimizado	• En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización. • Se utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales.

	• La entidad genera tráfico en IPv6.

Tabla No 2. Características de los Niveles de Madurez

8. ROLES Y RESPONSABILIDADES

A nivel general los funcionarios y contratistas de la **Instituto de Patrimonio y Cultura de Cartagena - IPCC** asumirán los siguientes roles y responsabilidades, una vez se formalice el MSPI al interior de la Entidad.

9. COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

- Aprobar y verificar del cumplimiento del Modelo de Seguridad y Privacidad de la Información, al interior de la entidad.
- Ser consciente de la criticidad de los activos de información para el desarrollo de los procesos de la Entidad.
- Divulgar las responsabilidades de seguridad y privacidad de la información de la entidad con base en los lineamientos del MSPI.
- Asignar los recursos necesarios para la implementación del MSPI alinterior de la Instituto de Patrimonio y Cultura de Cartagena - IPCC.

10. LÍDER DE PROCESO

- Liderar y apoyar la mejora continua del proceso, para la aplicación del MSPI.
- Alinear el proceso con los objetivos institucionales, con el fin de que su cumplimiento este apoyado por el MSPI.

- Asignar y verificar el cumplimiento de las funciones y responsabilidades de seguridad y privacidad de la información para los roles que actúan en el proceso.
- Apoyar la capacitación y entrenamiento requerido para que los
- funcionarios y contratistas que actúan en el proceso.
- <Aplicar el proceso disciplinario ante los incidentes de seguridad y privacidad de la información originada por un funcionario o contratista que actúan en el proceso.

11. LÍDER DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Liderar y apoyar la mejora continua para la aplicación del MSPI al interior de la Instituto de Patrimonio y Cultura de Cartagena - IPCC.
- Asignar dentro de su equipo de trabajo quien servirá como oficial de seguridad y privacidad de la información.
- Apoyar las actividades relacionadas con el MSPI.

12. OFICIAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Apoyar en definir y actualizar el inventario de los activos de información.
- Realizar análisis de riesgos de seguridad y privacidad de la información con base en lo establecido en el MSPI.
- Apoyar en definir del plan de tratamiento de los riesgos de seguridad y privacidad de la información.
- Velar por la ejecución del plan de tratamiento de los riesgos de seguridad y privacidad de la información.
- Definir, actualizar y difundir las políticas, procedimientos y formatos delMSPI.
- Definir y generar las métricas de seguridad y privacidad de la información establecida en el MSPI.
- Propender una cultura de seguridad y privacidad de la información al interior de la entidad.

- Lo anterior es responsabilidad del oficial de seguridad y privacidad de la información, pero debe contar con la participación de todos los funcionarios y contratistas del **IPCC.**

13. MESA DE TRABAJO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Validar y actualizar la documentación propia del MSPI dentro de la dependencia que representa.
- Fomentar dentro de su dependencia la práctica de directrices de seguridad y privacidad de información.
- Apoyar la identificación y actualización del inventario de activos de información y riesgos de estos.
- Apoyar la identificación e implementación de controles para lamitigación de riesgos de seguridad y privacidad de información.
- Participar en las jornadas de implementación, mantenimiento y mejora del MSPI.

14. FUNCIONARIOS Y CONTRATISTAS

Todos los funcionarios y contratistas vinculados al IPCC tendrán la responsabilidad de velar por la confidencialidad, integridad, disponibilidad y privacidad de la información que maneje, así mismo debe reportar los incidentes de seguridad, eventos sospechosos o un mal uso de los recursos que identifique.

El incumplimiento a la política general de seguridad y privacidad de la información traerá consigo, las consecuencias legales que apliquen a la normativa de la entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

15. TÉRMINOS Y DEFINICIONES

Para efectos de entendimiento de la presente política general seguridad y privacidad de la información, es importante tener en cuenta los siguientes términos y definiciones:

- **Acceso remoto**: conexión con los recursos informáticos de la entidad desde una ubicación remota a través de una red pública.
- **Activos de información**: son aquellos recursos con los que cuenta una empresa. Es decir, todo elemento que compone el proceso completo de comunicación, partiendo desde la información, el emisor, el medio de transmisión y receptor.
- **Amenaza:** causa potencial de incidente no deseado, el cual puede resultar en daño al Sistema o a la Organización. [Fuente: ISO 27000].
- **Brecha**: se denomina al espacio o ruta a recorrer entre un estado actual y un estado deseado.
- **Calidad**: es la cualidad de un conjunto de información recogida, que reúne entre sus atributos la exactitud, completitud, integridad, actualización, coherencia, relevancia, accesibilidad y confiabilidad necesarias para resultar útiles al procesamiento, análisis y cualquier otro fin que un usuario quiera darles.
- **Confidencialidad:** propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados, asegurando el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.
- **Conservación:** mantener y cuidar la información para que no pierda sus características y propiedades con el paso del tiempo.
- **Disponibilidad:** característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- **Dispositivo móvil:** son todos los equipos tecnológicos que acceden a Internet, tales como: portátiles, teléfonos IP, celulares, TV, tabletas, entre otros.
- **Entrenamiento**: proceso utilizado para enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo u objeto contractual.
- **Equipos de cómputo:** se reconoce como los portátiles o computadores de escritorios que se le asigna a un funcionario o contratista de la entidad.
- **Estándar:** regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

- **Información:** conjunto organizado de datos generados, obtenidos, adquiridos, transformados o controlados que constituyen un mensaje sin importar el medio que lo contenga (digital y no digital).
- **Ingeniería social:** técnica que utilizan las personas para obtener información, acceso o privilegios en sistemas de información, permitiendo que algún acto perjudique o exponga a la persona o entidad.
- **Integridad:** propiedad que busca mantener los datos libres de modificaciones no autorizadas. A grosso modo, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
- **Monitoreo**: verificación, supervisión, observación crítica o determinación continua del estado con el fin de identificar cambios con respecto alnivel de desempeño exigido o esperado.
- **MSPI:** Modelo Seguridad y Privacidad de la Información.
- **Política:** declaración de alto nivel que describe la posición de la entidad sobre un tema específico.
- **Privacidad de la información:** es el aspecto que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos pueden ser compartidos con terceros.
- **Procedimiento:** define específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada.
- **Propietario del activo:** persona o cargo que administra, autoriza el uso, regula o gestiona el activo de información. El propietario del activo aprueba el nivel de protección requerido frente a confidencialidad, integridad y disponibilidad.
- **Riesgo:** efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización). [Fuente: ISO 31000]
- **Sensibilización**: es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.
- **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información. NTC-ISO/IEC 27001.

- **Teletrabajo:** En Colombia, el teletrabajo se encuentra definido en la Ley 1221 de 2008 como: “Una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios terceros utilizando como soporte las tecnologías de la información y comunicación -TIC- para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio especifico de trabajo”.
- **TIC:** Tecnologías de la Información y Comunicaciones.
- **Vulnerabilidad:** debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información.