PLAN ESTRATEGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2024

OFICINA DE SISTEMAS ICULTUR

VERSIÓN 1.0

Cartagena de Indias 2024

Contenido

1. GENERALIDADES DEL PLAN INSTITUCIONAL

1.1. INTRODUCCIÓN

Para efectos de este documento, se entiende por lineamiento, la directriz o disposición que debe ser implementada por las entidades públicas para el desarrollo de la política de seguridad y se desarrollan a través de estándares, guías, recomendaciones o buenas prácticas.

La dirección de Tecnologías y Sistemas de Información o quien haga sus veces en las entidades del orden nacional y territorial, deben realizar el análisis y gestión de los riegos asociados a su infraestructura tecnológica haciendo énfasis en aquellos que puedan comprometer la seguridad de la información o que puedan afectar la prestación del servicio de TI.

1.2. ALCANCE

El Plan estratégico de seguridad y privacidad de la información,busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Implementar un Plan Estratégico de Seguridad y Privacidad de la Información acorde con los lineamientos del habilitado de seguridad y privacidad de la política de gobierno digital en el instituto distrital de deporte y recreación de Cartagena.

1.3.2. OBJETIVOS ESPECÍFICOS

- Realizar un diagnóstico del estado actual de la gestión de seguridad y privacidad de la información al interior del Instituto de Cultura y Turismo de Bolivar.(ICULTUR)
- Promover el uso de mejores prácticas de seguridad de la información, para que constituya la base de aplicación del concepto de Seguridad Digital.
- Dar lineamientos para la implementación de mejores prácticas de seguridad que permitan la identificación de infraestructuras críticas en la entidad.
- Contribuir con la mejora de los procesos de intercambio de información pública, las prácticas en seguridad y privacidad y la optimización de la gestión de la seguridad de la información al interior de la entidad.
- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la Información, Seguridad Digital y protección de la información personal.
- Orientar a la entidad en la transición del protocolo lPv4 a IPv6 con la utilización de las guías disponibles y en la adopción de la legislación relacionada con la protección de datos personales.
- Contribuir en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones, el ejercicio de arquitectura empresarial apoyado en el cumpliendo de los lineamientos del marco de referencia de arquitectura TI del Estado colombiano.

- Optimizar la labor de acceso a la información pública al interior de las entidades destinatarias y la revisión de los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para la optimización de su articulación.

2. CONTEXTO ESTRATÉGICO

El contexto estratégico del Plan de Seguridad y Privacidad de la información se refiere a cómo la organización maneja y protegen la información confidencial y privada de sus contratistas, empleados y otros grupos de interés. Esto incluye la implementación de medidas de seguridad física y digital, la creación de políticas y procedimientos para el manejo de la información, y la educación y concientización de los empleados sobre los riesgos de privacidad y seguridad. Además, las organizaciones deben cumplir con las normatividad y regulaciones aplicables en materia de privacidad y seguridad de la información.

Durante la vigencia 2021 se elaboraron la política general de Seguridad l y los manuales de políticas de seguridad.

En esta misma línea se pretende seguir robusteciendo este Proceso, mediante la elaboración de otros Procedimientos, formatos y guías que aborden la totalidad de los servicios TI, prestados por la entidad. Por esto se hace necesario la ejecución de la herramienta de autoevaluación MSPI para establecer las brechas y establecer planes acciones correspondientes.

3. CONTEXTO ORGANIZACIONAL

Para el desarrollo de las organizaciones, en términos de calidad de acuerdo a los lineamientos del Departamento Administrativo de Función Pública DAFP, según la Guía para la Gestión por Procesos en el Marco del Modelo Integrado de Planeación y Gestión MIPG versión 1, es la adopción de una gestión por procesos, permitiendo la mejora sustancial de las actividades al interior de las Entidades Públicas, orientando sus esfuerzos al servicio de los grupos de interés y de valor, permitiendo dar resultados acordes a las necesidades de estos.

del Comité Institucional de Gestión y Desempeño, actualizó su Mapa de Procesos, permitiendo con esto lograr aunar esfuerzos en procura de generar valor a través de la gestión por procesos, impactando al ciudadano como eje fundamental de la Gestión Pública.

4. MARCO CONCEPTUAL

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 MSPI.

ATAQUE: Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.

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

CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN: Procesos y procedimientos para garantizar una operativa continuada de la seguridad de la información.

CONTROL: Medida por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguardan o contramedida son utilizados frecuentemente como sinónimos de control.

CRITERIO DEL RIESGO: Los criterios del riesgo se basan en los objetivos de la organización y el contexto externo y el contexto interno. Los criterios de riesgo pueden derivarse de estándares, leyes, políticas y otros requisitos.

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible

violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

FIABILIDAD: Propiedad del comportamiento y de unos resultados consistentes previstos.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

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

ISO/IEC 27001: 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.

ORGANIZACIÓN: Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.

PROFESIONAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI): Persona que establece, implementa, mantiene y mejora continuamente uno o más procesos del sistema de gestión de seguridad de la información.

RECURSOS DE TRATAMIENTO DE INFORMACIÓN: Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

RENDIMIENTO: El rendimiento puede relacionarse con hallazgos cuantitativos o cualitativos. El rendimiento puede relacionarse con la gestión de actividades, procesos, productos (incluidos servicios), sistemas u organizaciones.

REQUISITO: Necesidad o expectativa que es establecida, generalmente de forma implícita u obligatoria.

RIESGO: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado: positivo o negativo. La incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o probabilidad.

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SISTEMA DE INFORMACIÓN: Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes que manejan información.

TRAZABILIDAD: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. MARCO NORMATIVO

Norma	Tema
Decreto 1008 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.
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”

Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
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.
Decreto 1078 de 2015	Por el cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, el cual incluye el Decreto 2573 de 2014, el cual establece los lineamientos generales de la Estrategia de Gobierno en Línea.
CONPES 3854 de 2016 **CONPES 3701 de 2011.** **CONPES 3905 de 2020.**	Política Nacional de seguridad Digital. Lineamientos de Política para Ciberseguridad y Ciberdefensa. Política Nacional de Confianza y Seguridad Digital.
Ley 1581 de 2012	Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales.
ISO 27001	Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los

	sistemas que la procesan.
RESOLUCIÓN No.500 DE MARZO 10 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

6. DESCRIPCIÓN DEL PLAN

Un plan de privacidad y seguridad de la información es un conjunto de medidas y procedimientos diseñados para proteger la privacidad y seguridad de la información confidencial de una organización. El plan debe incluir medidas para prevenir, detectar y responder a incidentes de privacidad y seguridad de la información, así como cumplir con las leyes y regulaciones aplicables en materia de privacidad y seguridad de la información.

Para la gestión de este plan se tienen en cuenta actividades que impacten en los siguientes aspectos del MSPI:

- Identificación y evaluación de riesgos: Un análisis de los riesgos potenciales para la privacidad y seguridad de la información, incluyendo los riesgos internos y externos.
- Políticas y procedimientos: Un conjunto de políticas y procedimientos para garantizar que la información se maneja de manera segura y cumpliendo con las regulaciones aplicables
- Medidas de seguridad física y digital: medidas de seguridad para proteger la información física y digital, tales como protección de la infraestructura, firewalls, encriptación, autenticación de usuarios, etc
- Educación y concientización: Capacitaciones a los empleados sobre la privacidad y seguridad de la información, incluyendo temas como el manejo seguro de contraseñas, el uso seguro de dispositivos móviles, y cómo identificar y responder a incidentes de seguridad.
- Monitoreo y auditorías: Monitoreo y auditorías regulares para detectar y responder a incidentes de privacidad y seguridad de la información.
- Plan de respuesta a incidentes: Un plan detallado para responder a incidentes de privacidad y seguridad de la información, incluyendo un plan de comunicación con los interesados afectados.

7. METODOLOGÍA DE SEGUIMIENTO

Para el correcto seguimiento del Plan de Seguridad y Privacidad de la Información al interior de la entidad, se construirán unos indicadores de gestión que permitirán establecer el avance de cumplimiento a partir de actividades planeadas para cada uno de los componentes que conforman el presente plan institucional.

Es de precisar que las actividades a desarrollar son apuestas al mejoramiento de los procesos dentro de la entidad en términos de transparencia, acceso a la información y lucha contra la corrupción.

7.1. PLAN DE ACCIÓN.

Se estableció la herramienta Plan de Acción como criterio documental para la gestión del Plan de Seguridad y Privacidad de la Información, ya que enmarca la hoja de ruta a seguir en la ejecución del plan.

Esta herramienta administrativa establece la ruta a implementar para gestionar los productos o metas necesarias para el cumplimiento de los objetivos en el marco de la misionalidad de la entidad.

7.2. BATERÍA DE INDICADORES

En el marco de la **Guía para la Construcción y Análisis de Indicadores 2018** del Departamento Nacional de Planeación DNP, que orienta en la construcción y análisis de los indicadores a partir de la **CADENA DE VALOR** (relación secuencial y lógica entre insumos, actividades, productos y resultados en la que se añade valor a lo largo del proceso de transformación total)[1]de la entidad.

Con relación a la Cadena de Valor de la entidad, los indicadores a utilizar son los **INDICADORES DE GESTIÓN**, cuyo objetivo principal es cuantificar y medir dos elementos.

- La cantidad de insumos utilizados.
- Las acciones de gestión realizadas.

[1](DNP, 2017, pág. 5)

Teniendo en cuenta los tipos de indicadores de gestión, se establecen indicadores de eficacia, eficiencia y efectividad, con relación al desarrollo de las actividades dentro del Plan de Acción del Plan Institucional.

EFICACIA: Grado en el que se realizan las actividades planificadas y se alcanzan los resultados planificados.[2]

EFICIENCIA: Medida en que el uso de los insumos (recursos financieros, humanos, técnicos y materiales) se ha hecho en forma económica u óptima para generar productos. Relación entre el resultado alcanzado y los recursos utilizados.[3]

EFECTIVIDAD: Medida del impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles.[4]

Los Indicadores de gestión del Plan de Seguridad y Privacidad de la Información son los siguientes:

1. **Nombre del Indicador:** Grado de implementación de normativas y controles de acuerdo con la política de Seguridad Digital

   Tipo de indicador: Eficacia

   Objetivo del Indicador: Determinar el porcentaje de cumplimiento de implementación de normativas y controles de acuerdo a la política de Seguridad Digital.

   Formula de Calculo:

$$Eficacia = \frac{No\ de\ Actividades\ realizadas}{No\ de\ Actividades\ Programadas} x100$$

2. **Nombre del Indicador:** Grado de satisfacción y apropiación del proceso Gestión TIC

   Tipo de indicador: Eficiencia

   Objetivo del Indicador: Determinar el porcentaje de satisfacción y apropiación del proceso Gestión TIC en materia de Seguridad Digital.

   Formula de Calculo:

[2]Glosario- Servicio al Ciudadano – Función Pública.
[3] Glosario- Servicio al Ciudadano – Función Pública.
[4]Glosario- Servicio al Ciudadano – Función Pública.

$$Eficiencia = \frac{No\ de\ solicitudes}{No\ de\ solicitudes\ atendidas} x100$$

7.3. CRONOGRAMA DE SEGUIMIENTO Y EVALUACIÓN

Para el seguimiento y evaluación del Plan de Acción, se debe realizar una evaluación trimestral y las fechas programadas para la entrega de informes, con el fin de dar cumplimiento a los compromisos, son:

SEGUIMIENTO	Entrega Informe de Gestión Plan Institucional
I Trimestre	Abril
II Trimestre	Julio
III Trimestre	Octubre
IV Trimestre	Diciembre

7.4. MEDICIÓN TRIMESTRAL DE METAS

Con el fin de medir la **EFICACIA** del Plan Institucional de Seguridad y Privacidad de la Información, se definieron rangos de seguimiento para medir la gestión del Plan de Acción, y establecer alertas y planes de choque que permitan el cumplimiento de lo planeado.

MATRIZ DE RANGOS PORCENTUALES DE GESTIÓN

Nivel de EFICACIA	Estado delIndicado	Marzo	Junio	Septiembre	Diciembre
ALTO		25% o más	50% o más	75% o más	95% o más
MEDIO		15% a 24,9%	40% a 49,9%	65% a 74,9%	85% a 94,9%
BAJO		Menos de 15%	Menos de 40%	Menos de 65%	Menos de 85%

8. CONTROL DE CAMBIOS

Versión	Fecha y número de Acta y/o Acto Administrativo aprobación	Elaborado por:	Revisado por:	Aprobado por:	Descripción del Cambio
1.0	Acta de Comité Institucional de Gestión y Desempeño No. ___-01-2024		Jefe Oficina Asesora de Planeación	Comité MIPG	Primera Versión.