PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CORPORACION DE CULTURA Y TURISMO DE ARMENIA

2023

INTRODUCCIÓN

En Colombia se viene adelantando la implementación de la política de gobierno digital, tal como lo establece el decreto 1008 de 2018, cuyas disposiciones se compilan en el Decreto Único Reglamentario del Sector TIC, 1078 de 2015, específicamente en el capítulo 1, titulo 9, parte 2, libro 2, como un instrumento fundamental para mejorar la gestión pública y la relación del estado con los ciudadanos, la cual se ha articulado con el Modelo Integrado de Planeación y Gestión, como una herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo, articulada a otras políticas esenciales para la gestión pública en Colombia.

El Manual de la política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones establece que la política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

Según el manual, la implementación de la política de gobierno digital se ha definido en dos componentes: TIC para el estado y TIC para la sociedad, que sonhabilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales. Estos cinco elementos, se desarrollan a través de lineamientos y estándares, que son requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar los logros de la política.

El manual en mención, precisa que el habilitador de seguridad de la información busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, tramites, servicios, sistemas de información,

infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Este habilitador se soporta en el Modelo de Seguridad y Privacidad de la información (MSPI). No obstante, el manual está amparado en el Decreto 1008 del 2018, que en su artículo 2.2.9.1.1.3 define que la política de Gobierno Digital se desarrollará conforme a los principios que rigen la función y los procedimientos administrativos adoptados en Colombia, en particular al principio de Seguridad dela Información, que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del estado, y de los servicios que prestan al ciudadano.

El documento denominado Modelo de Seguridad y Privacidad de la Información (MSPI), expedido por el Ministerio de Tecnologías de Información y de las Comunicaciones, expresa que la adopción del mismo, por las entidades del estado, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, apoyada en un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.
La adopción, implementación y evaluación del modelo mencionado, es una actividad obligatoria según lo expresado en el artículo 2.2.9.1.3.2., en el numeral 2, en los literales A, B y C, el cual debe ser planificado en atención a lo establecidoen el decreto 612 de 2018, que en el artículo 1, señala la importancia de la integración de los planes institucionales y estratégicos al Plan de Acción institucional, en el ámbito de aplicación del modelo integrado de planeación y gestión.

Así mismo, la resolución 0500 de marzo 10 del 2021 expedida por el Ministerio de Tecnologías de Información y de las Comunicaciones, que tiene como objeto establecer los lineamientos generales para la implementación del Modelo de

Seguridad y Privacidad de la Información, la guía de gestión de riesgos de Seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y establecer los lineamientos y estándares para la estrategiade seguridad digital. La resolución en mención precisa la necesidad de que los sujetos obligados deban adoptar las medidas técnicas, administrativas y de talentohumano para garantizar que la seguridad digital se incorpore al Plan de Seguridad y Privacidad de la Información y así mitigar los riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Es precisamente a través del artículo 5 de la resolución 0500 que se precisa la necesidad de adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital, e incluirla en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en lostérminos del artículo 2.22.22.3.14 del capítulo 3 del título 22 de la parte 2 del libro2 del decreto 1083 de 2015. En atención a lo anterior, se presenta el plan de seguridad y privacidad de la información enfocado en la seguridad informática frente a Ciberamenazas de activos de tecnologías de información de la entidad.

La adopción e implementación del Modelo de Seguridad y Privacidad de la información en las entidades públicas toma como sustento el estándar NTC ISO 27001:2013, así como principios regulatorios definidos por el Gobierno Nacional, tal como la Ley 1712 de 2014 o la Ley 1581 de 2012; así mismo, apoyan su enfoque en la implementación de un ciclo de identificación, valoración y tratamiento de riesgos de seguridad y privacidad de la información, para lo cual se ha expedido desde el Departamento Administrativo de la Función Pública la guía para la administración del riesgo y el diseño de controles en entidades públicas, como referente para abordar los riesgos de gestión, corrupción y de seguridad de la información. La adopción de prácticas de gestión de riesgos en las entidades públicas permitirá fortalecer la toma de decisiones en cuanto a la implementación de controles de acuerdo con el plan de tratamientos definido. Estos referentes constituyen el fundamento para la definición del plan de tratamiento de riesgos de seguridad y privacidad de la información con enfoque en la seguridad informática frente a Ciberamenazas sobre activos de tecnologías de información y de las comunicaciones del Centro de Datos Corporativo.

OBJETIVO GENERAL

Establecer un marco de acción para aportar al tratamiento de riesgos de seguridad y privacidad de la información, sobre los activos de tecnologías de información que soportan la prestación de servicios digitales de la Entidad, y establecer el Plan de Seguridad y Privacidad de la Información, el cual está dirigido a la implementación del modelo de seguridad y privacidad de la información MSPI y a todas las etapas que lo componen. Lo anterior en atención al contexto organizacional de la entidad, las capacidades técnicas y recursos disponibles.

OBJETIVOS ESPECÍFICOS

- Comunicar e implementar la estrategia de seguridad de la información.
- Identificar infraestructuras críticas en la entidad a través de la implementación de mejores prácticas de seguridad de la información.
- Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información – MSPI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
- Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios

AVANCES DE LA ENTIDAD EN EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Corporación de Cultura y Turismo de Armenia ha priorizado abordar la gestión de riesgos deseguridad informática sobre los activos de tecnologías de información frente a infraestructuras críticas y ciberamenazas. A enero de 2023, los activos de tecnologías de información registran 13 ítems de configuraciónregistrados (fuera de los contratistas que ingresan a la Entidad con sus equipos portátiles), de los cuales se consideraron 17 como activos de tecnologías deinformación de interés para el análisis realizado, en atención al papel que juegan en la prestación de servicios institucionales.

Con el propósito de facilitar la identificación de los activos de tecnologías de información registrados, se han agrupado en un conjunto de categorías

CANTIDAD DE ELEMENTOS DE CONFIGURACIÓN POR CATEGORÍAS	
CATEGORÍA DE ACTIVO DE TECNOLOGÍA DE INFORMACIÓN	**PORCENTAJE DE ELEMENTOS DE CONFIGURACIÓN**
ESTACIONES DE USUARIO FINAL (13)	76,4%
TELECOMUNICACIONES (1)	5,9%
SISTEMAS DE INFORMACIÓN (2)	11,8%
BASES DE DATOS (1)	5,9%
TOTAL	**17**

A partir de la agrupación se detalla que el 76.4% de los elementos de configuración se organizaron en el grupo de Estaciones de Usuario Final, que reúne los activos de tecnologías de información relacionados con equipos de cómputo y computadores portátiles; y el 5.9% se organizaron en el grupo de Telecomunicaciones, así como el 11.8% en el grupo de sistemas de información.

Una de las acciones relevante es la identificación de riesgos sobre los activos de tecnologías de información frente a infraestructuras críticas y Ciberamenazas, a partir de lo cual se define la siguiente matriz de riesgos:

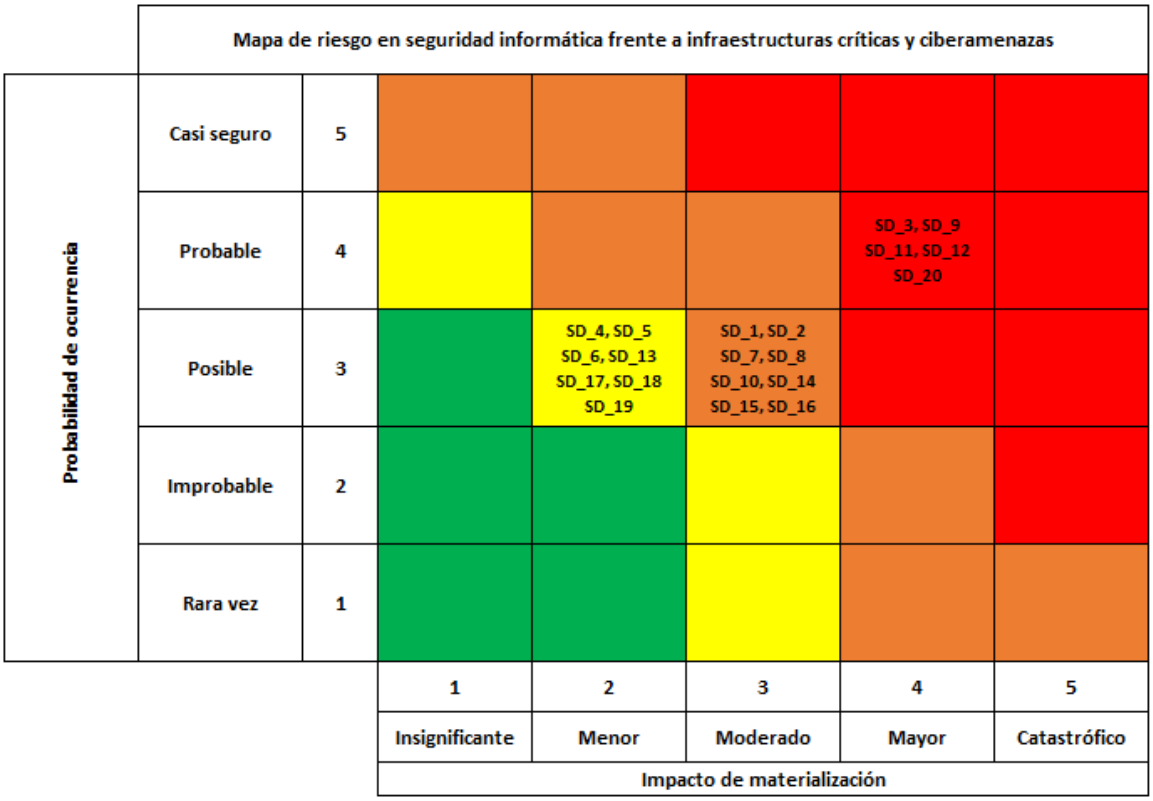
ID	Escenario de riesgo	Amenaza	Vulnerabilidad
SD_1	El desconocimiento de las Políticas para la seguridad de la información puede acarrear perdida de información de la Entidad.	Pérdida de información	[A.5.1.1] Se deben definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
SD_2	Utilización de equipos portátiles que se conectan a la red LAN de la Entidad	Potencial riesgo de ingreso de virus, Spyware, Malware, etc. proveniente de equipos externos, así como de unidades de almacenamiento externas	[A.6.2.1] Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
SD_3	Colaboradores no capacitados o indolentes frente a la seguridad de la información	Se pone en riesgo la integridad de la información de la Entidad tanto por acción como por omisión	[A.7.2.2] Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
SD_4	Violaciones a la seguridad de la información consciente o inconscientemente	Se pone en riesgo la integridad de la información de la Entidad tanto por acción como por omisión	[A.7.2.3] Se debe contar con un proceso disciplinario formal el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una

			violación a la seguridad de la información.
SD_5	Afectación de la disponibilidad, integridad o confidencialidad de los equipos de cómputo, por acción hackers, debido a una falta o deficiencia en controles de seguridad informática en la gestión de las redes	Pérdida, modificación o destrucción no autorizada de la información	[A.9.1.2] Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
SD_6	Control de acceso a sistemas y aplicaciones	Pérdida, modificación o destrucción no autorizada de la información	[A.9.4.1] El acceso a la información y a las funciones de los sistemas de las aplicaciones se deberá restringir de acuerdo con la política de control de acceso.
SD_7	Afectación de la disponibilidad, integridad o confidencialidad de los servidores, por acción hackers, debido a una falta o deficiencia en controles que garanticen el procedimiento de ingreso seguro de inicio de sesión	Hackers	[A.9.4.2] Falta o deficiencia en controles que garanticen el procedimiento de ingreso seguro de inicio de sesión sistemas de información
SD_8	Controles físicos de entrada	Pérdida, modificación o destrucción no autorizada de la información; así como la sustracción de bienes de la entidad	[A.11.1.2] Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
SD_9	Seguridad de oficinas, recintos e instalaciones	Pérdida, modificación o destrucción no autorizada de la información; así como la sustracción de bienes de la entidad	[A.11.1.3] Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
SD_10	Ubicación y protección de los equipos	Pérdida, modificación o destrucción no autorizada de la información; así como la sustracción de bienes de la entidad	[A.11.2.1] Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y

			las oportunidades para acceso no autorizado.
SD_11	Servicios de suministro	Pérdida de información por daño en equipos de cómputo	[A.11.2.2] Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
SD_12	Afectación de la disponibilidad, integridad o confidencialidad de los equipos de cómputo, por acción de Spyware/Malware, debido a una falta o deficiencia en controles sobre la detección, prevención, recuperación para proteger contra códigos maliciosos.	Spyware/Malware	[A.12.2.1] Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
SD_13	Respaldo de información	Daño irreversible o pérdida de medios de almacenamiento	[A.12.3.1] Se deben hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
SD_14	Instalación de software en sistemas operativos	Ingreso de software malintencionado	[A.12.5.1] Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
SD_15	Separación en las redes	Ataques externos	[A.13.1.3] Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
SD_16	Afectación de la disponibilidad, integridad o confidencialidad de los sistemas de información web, por acción de hackers, debido a una falta o deficiencia en controles que garanticen el adecuado análisis y especificación de requisitos de	Atacante interno(insider)	[A.14.1.1] Falta o deficiencia en controles que garanticen el adecuado análisis y especificación de requisitos de seguridad

	seguridad informática en los sistemas de información		informática en los sistemas de información
SD_17	Análisis y especificación de requisitos de seguridad de la información	Ataques externos	[A.14.1.1] Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
SD_18	Desarrollo contratado externamente	Ataques externos	[A.14.2.7] La Entidad debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
SD_19	Política de seguridad de la información para las relaciones con proveedores	Pérdida, modificación o destrucción no autorizada de la información	[A.15.1.1] Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la Entidad.
SD_20	Implementación de la continuidad de la seguridad de la información	Desastre natural o conflicto armado	[A.17.1.1] La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

A continuación, se presenta el mapa de riesgos producto de la aplicación de los controles identificados de la aplicación de los controles a los riesgos inherentes, así como de los controles sobre los riesgos residuales identificados, en el que se identifican el conjunto de riesgos frente a la probabilidad de ocurrencia y el impacto de la materialización, tal como se puede evidenciar en la siguiente gráfica:



No obstante, la Entidad es consciente que la gestión de riesgos de dinámica y que la revisión, actualización y reevaluación es parte de un ciclo que redunda en aportar al mejoramiento de la seguridad de la información corporativa.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE ACTIVOS DE TECNOLOGÍAS DE INFORMACIÓN

Según lo expuesto en la guía para la administración del riesgo y el diseño de controles en entidades públicas por el Departamento Administrativo de la Función Pública, el tratamiento de riesgos es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, por lo tanto dicha planeación en este caso en particular, hace alusión al tratamiento de riesgos de seguridad y privacidad de la información enfocado en la seguridad informática sobre los activos de tecnologías de información frente a Ciberamenazas, para lo cual se realizan unas actividades durante la vigencia orientadas a implementar los controles requeridos y priorizados. En atención a lo anterior, a continuación, se describen las actividades más relevantes orientadas al tratamiento de riesgos de seguridad y privacidad de la información desde el enfoque de seguridad informática frente a infraestructuras críticas y Ciberamenazas:

PLAN DE ACCION DEL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN				
NO.	**DESCRIPCIÓN DE LA ACTIVIDAD**	**RESPONSABLE**	**TIEMPO**	
1	Establecer un plan de capacitaciones a todos los funcionarios sobre la política de seguridad y privacidad de la información	Oficina TIC o quien haga sus veces	Febrero de 2023	Diciembre de 2023
2	Implementar controles de detección, de prevención y de recuperación, para proteger contra códigos maliciosos.	Oficina TIC o quien haga sus veces	Febrero de 2023	Diciembre de 2023

3	Adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	Oficina TIC o quien haga sus veces	Febrero de 2023	Diciembre de 2023
4	Establecer controles de acceso a los sistemas de información y a los equipos	Oficina TIC o quien haga sus veces	Febrero de 2023	Diciembre de 2023
5	Establecer controles para el acceso a los espacios físicos de la Entidad	Dirección	Febrero de 2023	Diciembre de 2023
6	Establecer los mecanismos para evitar fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro, para la protección de los equipos.	Dirección, Oficina TIC o quien haga sus veces	Febrero de 2023	Diciembre de 2023
7	Implementar el proceso para realizar copias de seguridad periódicas	Oficina TIC o quien haga sus veces	Febrero de 2023	Diciembre de 2023
8	Implementar acciones que eviten la instalación de software sin autorización	Oficina TIC o quien haga sus veces	Febrero de 2023	Diciembre de 2023
9	Establecer todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la Entidad.	Dirección	Febrero de 2023	Diciembre de 2023
10	Establecer requisitos y acciones para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	Dirección, Oficina TIC o quien haga sus veces	Febrero de 2023	Diciembre de 2023

El desarrollo de las actividades para lograr su consecución estará sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; de acuerdo con la disponibilidad presupuestal oportuna, a las orientaciones de la alta dirección, en cuanto al deseo de contrarrestar el riesgo corporativo que han adoptado para afrontar el desarrollo y cumplimiento de las actividades planificadas.