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

1. Introducción

La información es un activo de alto valor para la Empresa de Parques y Eventos de Antioquia - **ACTIVA**. A medida que los procesos de la entidad se hacen más dependientes de la información y de las tecnologías que la soportan, se hace necesario contar con actividades de planeación estratégica que, en concordancia con la política de seguridad de la información institucional, permitan el tratamiento (principalmente la mitigación) riesgos y la atención a las necesidades de seguridad de la información de la entidad. El presente documento indica de forma general el tratamiento, es decir, las actividades para mitigar los riesgos identificados de seguridad de la información, así como también, las actividades para atender los requerimientos institucionales de seguridad de la información.

Se describe las actividades necesarias para llevar a cabo la identificación de riesgos de seguridad digital sobre los activos de información, la creación de controles y planes de mejora con su debido seguimiento para aplicar el correspondiente tratamiento de riesgos enmarcado en las siguientes categorías:

Aceptar el riesgo: la entidad decide después de un análisis no adoptar ninguna medida que afecte la probabilidad o el impacto del riesgo. Esta opción se puede considerar para riesgos con nivel bajo, sin embargo, se pueden presentar riesgos con otro nivel a los cuales la entidad no puede aplicar controles o planes para reducir el riesgo y es necesario aceptarlo. La aceptación del riesgo no implica que se olvide, sino que se debe hacer un seguimiento continuo del mismo.

Reducir el riesgo: se generan controles y/o planes de mejora que permitan reducir la probabilidad y/o el impacto del riesgo, estos controles están relacionados con la implementación de la ISO/IEC 27002, los cuales permiten una segregación de funciones, registros, entre otros que permitan la reducción prevista sobre el riesgo.

Evitar el riesgo: en este caso la entidad deja de realizar las actividades que dan lugar al riesgo.

Compartir el riesgo: en este caso existen dos maneras de compartir el riesgo y es tercerizar la operación de la actividad que conlleva la probabilidad del riesgo y la otra manera es por medio de la adquisición de un seguro.

2. Marco Legal

NORMA	DESCRIPCIÓN
Ley 1712 de 2014	“Ley de transparencia y del derecho de acceso a la información pública nacional”.
Ley 1581 de 2012 y decreto 1377 de 2013.	“Ley de transparencia y del derecho de acceso a la información pública nacional”.
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”.
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 04 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”.
NTC/ISO 31000:2009	Gestión del Riesgo. Principios y directrices.
NTC/ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).

3. Alcance

El plan de tratamiento de riesgos de seguridad y privacidad de la información será aplicado a los procesos estratégicos, misionales, de apoyo y de evaluación en la Empresa de Parques y Eventos de Antioquia – ACTIVA y deberá ser conocido y cumplido por todos los funcionarios, contratistas, proveedores, ciudadanía en general y demás partes interesadas, que accedan a los sistemas de información e instalaciones físicas.

4. Objetivo General

Establecer y dar a conocer el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información de ACTIVA.

4.1. Objetivos Específicos

- Identificar, monitorear y hacer seguimiento a los riesgos a que está expuesta la información, con el fin de establecer metodologías que permitan una adecuada administración de éstos.
- Comprometer a todos los que tienen acceso a la información con la formulación e implementación de medidas de seguridad en pro de la prevención y administración de los riesgos.
- Realizar seguimiento de los planes de manejo para el tratamiento de los riesgos.

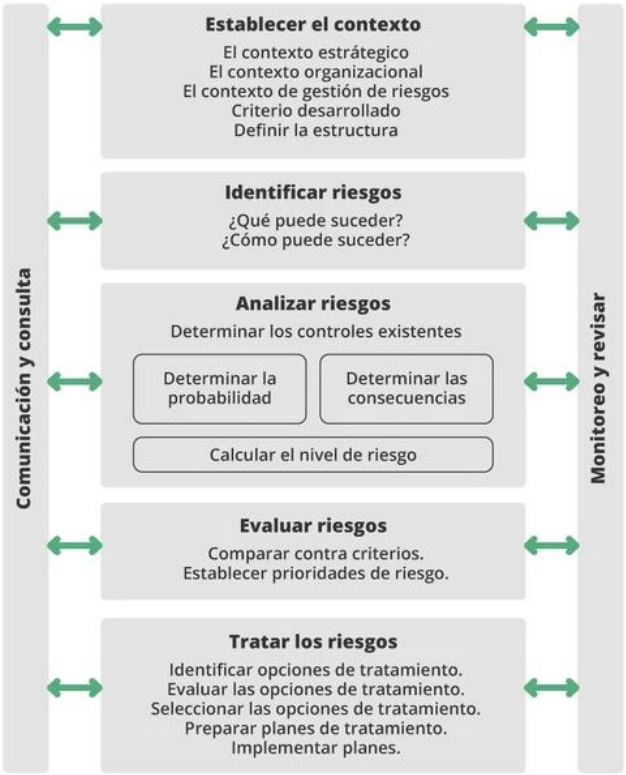
5. Partes Interesadas

Todos los funcionarios, contratistas, proveedores, entes de control, entidades gubernamentales del orden nacional, departamental y local, y ciudadanía en general que accedan a los sistemas de información e instalaciones físicas la Empresa de Parques y Eventos de Antioquia – ACTIVA

6. Desarrollo del plan

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en la Empresa de Parques y Eventos de Antioquia - ACTIVA, se toma como base las etapas de la Gestión a lo largo del MSPI, la cual será desarrollada a través de la ejecución de las actividades propuestas en el numeral 6.2.

6.1. TRATAMIENTO DEL RIESGO



La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso de MSPI.

ETAPAS DEL MSPI	PROCESO DE GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN
PLANEAR	Establecer el contexto Valoración del riesgo Planificación del tratamiento del riesgo Aceptación del riesgo
IMPLEMENTAR	Implementación del plan de tratamiento de riesgo
GESTIONAR	Monitoreo y revisión continua de los riesgos
MEJORA CONTINUA	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información

Tabla: Etapas de la Gestión a lo largo del MSPI

6.2. Actividades de Implementación 2024

ESTRATEGIA	ACTIVIDADES
Gestión de la Seguridad de la Información	Mejora del esquema de gestión de seguridad de la información institucional, buscando el cumplimiento del MSPI y la norma internacional de gestión ISO/IEC 27001
Toma de conciencia	Transmisión de mensajes enfocados en actuaciones correctas y responsables frente a la seguridad de la información por parte de los servidores y usuarios de la información institucional.
Diagnósticos externos y pruebas de concepto	Identificación y evaluación de tecnologías de seguridad de la información que podrían ser usadas para el tratamiento de riesgos de ciberseguridad.
Seguridad digital	Identificación y tratamiento de riesgos de seguridad digital
Sensibilización	Socialización Gestión del Riesgos de Seguridad y Privacidad de la información
Mejoramiento	Actualización Plan Gestión de Riesgos Seguridad de la Información, de acuerdo a los cambios solicitados

7. Seguimiento del plan

El área encargada de realizar el monitoreo, seguimiento y control del plan de acuerdo con la competencia y la normatividad vigente es el área de TI.

8. Terminología

Los siguientes términos son utilizados en el contexto de la gestión de la seguridad de la información y aplican para todas sus fases y momentos, incluyendo la gestión de riesgos.

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado. Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000)

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo. 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.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos

de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

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

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico. Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo. Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos. Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas que apuntan a un objetivo o que interactúan para transformar una entrada en salida.

Riesgo en la seguridad de la información: 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.

9. Control de Cambios

Versión	Fecha de Aprobación	Descripción del Cambio
01	31/01/2024	Creación del documento