PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. Introducción

El Plan de Seguridad de la Información es esencial para el Modelo de Seguridad y Privacidad de la Información (MSPI) en el contexto de Gobierno Digital. Este plan se basa en las directrices del Ministerio de Tecnologías de la Información y Comunicaciones, integrando las mejores prácticas para el diagnóstico, planificación, implementación, gestión y mejora continua. Se enfoca en las necesidades específicas, objetivos de seguridad, procesos clave y la estructura de la empresa ACTIVA de Antioquia. Al implementar este plan, ACTIVA cumple con el decreto 1078 de 2015, abordando la seguridad y privacidad de la información como un aspecto crucial de la estrategia de Gobierno Digital. Las políticas establecidas en este plan son fundamentales para implementar controles efectivos en la gestión de la información de ACTIVA.

2. Marco Legal

NORMA	DESCRIPCIÓN
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
NTC/ISO 27002:2013	Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.
Modelo Nacional de Gestión de Riesgos de Seguridad Digital.	Modelo Nacional de Gestión de Riesgos de Seguridad Digital.
Conpes 3701 del 14 de julio de 2011	Lineamientos de Política para Seguridad y Ciberdefensa.
Resolución 500 del 10 de marzo 2021	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.

3. Alcance

Todas las políticas de seguridad de la información, aquí contenidas, serán aplicadas y deberán ser conocidas y cumplidas por todos los funcionarios, contratistas y demás partes interesadas, asociados al proceso de Tecnología en la compañía.

4. Direccionamiento Estratégico

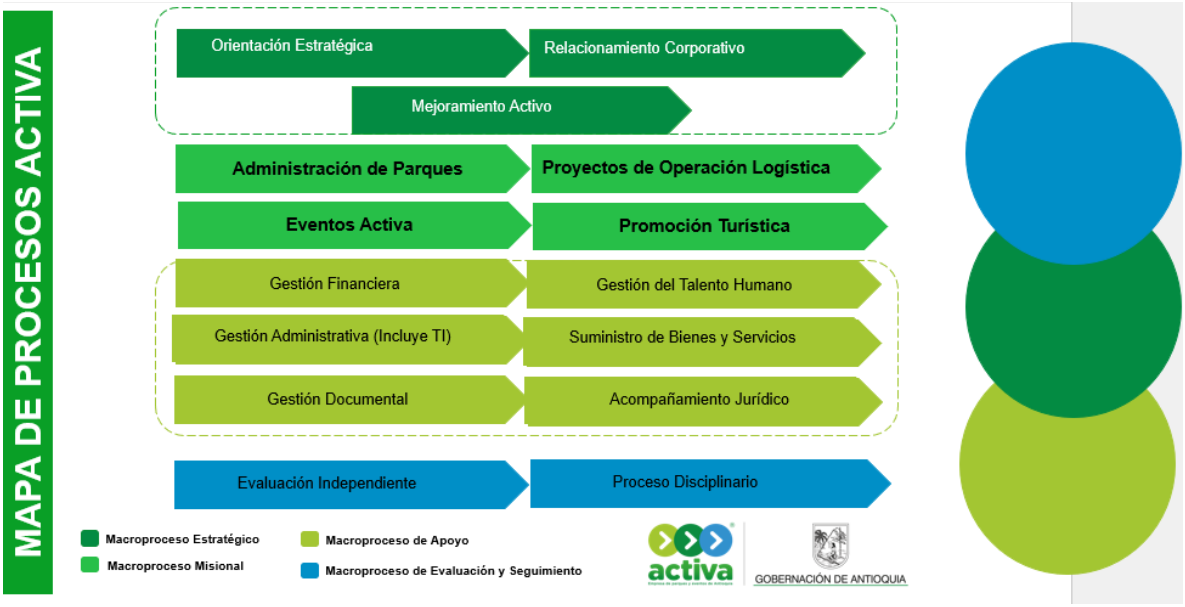
- **Misión**

Ofrecer soluciones completas en la gestión logística y operativa de parques, buscando enriquecer la vida de la comunidad antioqueña. Nos dedicamos a integrar tecnología e innovación en nuestras operaciones, contribuyendo así al desarrollo y bienestar socioeconómico de la región de Antioquia.

- **Visión**

Activa se posicionará como una empresa líder en eficiencia y rentabilidad. Nos proyectamos como una opción destacada en el mercado para la organización de eventos y la promoción de Antioquia. Nuestra visión se fundamenta en una estructura organizacional ágil y efectiva, un profundo conocimiento del mercado y la capitalización de avances tecnológicos para potenciar nuestras operaciones.

- **Mapa de Procesos**



5. Términos y Definiciones

Ataque DDoS (Distributed Denial of Service): Un intento de hacer que un sistema o red sea inaccesible para sus usuarios previstos sobrecargándolo con tráfico de varias fuentes.
Ataque de phishing: Un intento de adquirir información sensible haciéndose pasar por una entidad confiable en una comunicación electrónica.
Ataque de spear phishing: Una forma de ataque de phishing que se dirige específicamente a un individuo o empresa.
Ataque de ransomware: Un tipo de malware que restringe el acceso a un sistema informático hasta que se pague un rescate.
Ataque de man-in-the-middle (MitM): Un ataque donde el comunicador está bajo la impresión de que está comunicándose directamente con un cierto partido, pero en realidad toda la comunicación está siendo controlada por un tercero.
Ataque de día cero (Zero day): Un ataque que se aprovecha de una vulnerabilidad de software que es desconocida para aquellos que deberían estar interesados en corregirla.
Botnet: Una red de computadoras privadas infectadas con software malicioso y controladas como un grupo sin el conocimiento de sus dueños.
Malware: Software diseñado para interferir con un sistema informático o para recoger información confidencial.
Virus informático: Un tipo de malware que, cuando se ejecuta, se replica al modificar otros programas informáticos e insertar su propio código.
Gusano informático: Un malware que se propaga a través de una red sin la intervención del usuario.
Spyware: Software que permite a un usuario obtener información encubierta sobre las acciones de otro usuario.
Exploit: Un pedazo de software, un fragmento de datos, o una secuencia de comandos que aprovecha un defecto o vulnerabilidad para causar un comportamiento no intencional o no deseado.
Firewall: Una parte de un sistema o red que está diseñada para bloquear el acceso no autorizado, mientras permite la comunicación autorizada.
Vulnerabilidad: Una debilidad que permite a un atacante reducir la disponibilidad, integridad y confidencialidad de un sistema.
Encriptación: El proceso de convertir información o datos en un código para prevenir el acceso no autorizado.
Breach o violación de seguridad: Un incidente en el que se expone información confidencial, protegida o sensible.
Spoofing: Técnica que se utiliza para ganar acceso no autorizado a computadoras, donde alguien se hace pasar por otro usuario al falsificar los datos y así obtener un beneficio ilegítimo

Amenaza cibernética: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado.
Riesgo: Es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas.
Seguridad informática: Comprende los métodos, procesos o técnicas para la protección de los sistemas informáticos (redes e infraestructura) y la información contenida en formato digital en estos medios.
SGSI: Gestión de Seguridad de la Información.
MSPI: El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, Integridad, disponibilidad de la Información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgo.

6. Objetivo General

Establecer las políticas de seguridad de la información para la administración en la Empresa de parques y eventos de Antioquia – ACTIVA, con el fin de cumplir con los requisitos de seguridad, definidos en el MSPI que ayudarán, mediante la implementación, a preservar la confidencialidad, integridad y disponibilidad de la información. De acuerdo a los lineamientos de buenas prácticas en Seguridad y Privacidad para las entidades de Estado, con el fin de regular la gestión de la seguridad de la información al interior de la entidad.

Nos enfocamos en salvaguardar la operatividad y continuidad de ACTIVA, asegurando que la información propia y de nuestros **stakeholders** esté protegida de la manera más robusta posible. Todo ello en consonancia con nuestros principios fundamentales de confianza y preservación de capital. Este compromiso con la seguridad y la eficacia operacional garantiza que todos los procedimientos y actividades se ejecuten de manera segura y eficiente, respaldando así la integridad de la organización y la satisfacción de las partes interesadas.

7. Partes Interesadas

Todos los funcionarios, contratistas y ciudadanía en general que accedan a los sistemas de información e instalaciones físicas de la Empresa de parques y eventos de Antioquia – ACTIVA.

Entregable	Responsable de actividad	Actividad	Periodicidad
Usuario - Clave	TI	Creación, activación e inactivación de usuarios	A demanda
Contratos	Área Administrativa y Financiera	Renovación de licenciamiento	Anual
Plataforma Acronis	24 HN	Realizar backups	Diario
Evidencia del seguimiento	24 HN	• Registros de Auditoría: Muestran cambios recientes en la configuración de seguridad. • Informes de Configuración: Documentan las configuraciones actuales y su cumplimiento con las políticas de seguridad establecidas. • Informes de Análisis de Malware: Resumen los incidentes de seguridad relacionados con archivos y las acciones tomadas. • Estadísticas de Filtrado de Email: Reportan correos electrónicos marcados como spam, phishing, o con adjuntos sospechosos. • Estadísticas de Seguridad Web: Muestran intentos de acceso a sitios web maliciosos y las acciones preventivas tomadas. • Registros de Tráfico del Firewall: Detallan el tráfico bloqueado o permitido, incluyendo intentos de intrusión.	Diario

		• Informes de Política de Dispositivos: Documentan el cumplimiento y las violaciones a las políticas de uso de dispositivos. • Registros de Actividad Web: Presentan un historial detallado del uso de la web dentro de la red. • Reportes de Cumplimiento de Políticas Web: Indican la adherencia a las políticas de uso de internet establecidas. • Informes de Implementación de Cifrado: Muestran dónde y cómo se está utilizando el cifrado en la organización. • Cifrado de Información: • Informes de Implementación de Cifrado: Muestran dónde y cómo se está utilizando el cifrado en la organización.	
Evidencia del seguimiento	24 HN	Mantenimiento preventivo y/o correctivo a equipos de cómputo	

8. Esquema del plan

El Plan de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la empresa de parques y eventos de Antioquia – ACTIVA con respecto a la protección de los activos de información que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

9. Desarrollo del Plan

ACTIVA, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y las acciones a implementar son:

• Minimizar el riesgo de los procesos digitales de la entidad.
• Cumplir con los principios de seguridad de la información.

• Mantener la confianza de los funcionarios, contratistas y terceros.
• Apoyar la innovación tecnológica.
• Implementar el sistema de gestión de seguridad de la información.
• Proteger los activos de información.
• Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
• Fortalecer la cultura de seguridad de la información en los funcionarios, contratistas y ciudadanía en general.
• Garantizar la continuidad del negocio frente a incidentes.

La Política de Seguridad que soportan el SGSI, considera los siguientes aspectos:

• La Empresa de parques y eventos de Antioquia - ACTIVA ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
• Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

La Empresa de parques y eventos de Antioquia - ACTIVA:

- Protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros.
- Protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- Protegerá su información de las amenazas originadas por parte del personal.
- Protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementará control de acceso a la información, sistemas y recursos de red.
- Garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- Garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- Garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- Garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Seguimiento al Plan

- El área de talento humano deberá informar al área de TI acerca de las novedades de ingreso o retiro que labora en la entidad, con el fin de asignar o eliminar los usuarios desde la administración del office 365 y sus respectivos permisos de acceso a la información.
- Implementar un proceso sistemático para la identificación y manejo de vulnerabilidades en software y hardware, incluyendo escaneos regulares y actualizaciones de seguridad
- Software, se garantiza la continuidad de los aplicativos que requieren renovación anual, con el fin de tener el licenciamiento legal y vigente.
- Generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores.
- Monitorear constantemente los aplicativos de seguridad de la información, Fortinet y antivirus Sophos, con el fin de detectar y corregir cualquier anomalía.
- El proveedor de servicios, deberá atender incidentes o requerimientos de los usuarios a través de canales como el correo electrónico. La generación de un tiquete de atención permite clasificar y responder según la prioridad del incidente. El área de TI de ACTIVA, se encargará de realizar dicho escalamiento al proveedor.
- Siempre que un usuario reciba una notificación del sistema sobre un posible riesgo detectado, se debe notificar inmediatamente al área de TI.
- Todos los funcionarios y contratistas deberán cambiar su contraseña de acceso a los diferentes sistemas de información con una frecuencia mínima de 3 meses.
- Los funcionarios y contratistas deberán notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.
- No se debe almacenar contraseñas en el navegador de Internet.
- Bloquear el equipo de cómputo tras abandonar el puesto de trabajo, mediante el uso de las teclas Ctrl + Alt + Supr o tecla Windows + L
- Apagar los equipos de cómputo al finalizar la jornada laboral.
- Solo está permitido el uso de aplicaciones autorizadas en los equipos de la empresa. La instalación de cualquier programa no autorizado debe ser solicitado por el área de TI para revisar su viabilidad de instalación.
- Todos los usuarios tendrán un identificador único (ID usuario), de manera que las actividades tengan trazabilidad.
- El uso de la red interna de la compañía solo podrá ser utilizada para fines profesionales.

- Realizar auditorías de seguridad, tanto internas como externas, de forma regular para evaluar y mejorar la efectividad de las políticas y prácticas existentes
- Para el uso de escritorio remoto, se debe utilizar exclusivamente Splashtop, garantizando seguridad avanzada, gestión centralizada y reportes detallados para un control óptimo del entorno de TI.
- Los equipos suministrados por ACTIVA como portátiles, dispositivos móviles, entre otros; no deben realizar alteraciones y /o modificaciones en su hardware.
- El contratista de servicio en Nube es el responsable de ejecutar la copia de respaldo de la información de la Empresa de parques y eventos de Antioquia.
- Se dispondrá de diferentes redes inalámbricas para el acceso de funcionarios, contratistas y visitantes.
- Las contraseñas al igual que los usuarios, no se deben compartir, todas las contraseñas deben tratarse como información sensible.
- Las contraseñas no deben ser almacenadas en formato legible, papeles, agendas de trabajo, computadores sin sistemas de control de acceso o cualquier otro lugar donde las personas no autorizadas puedan encontrarlas.
- Política del RACK: Prohibido el ingreso sin autorización previa.
- Se recomienda no consumir alimentos y/o líquidos en el puesto de trabajo.
- No se debe dejar notas al lado de la pantalla con contraseñas, información sensible y/o confidencial bajo el teclado, bajo el equipo o en ubicaciones accesibles.
- Todos los documentos que se trabajen compartidos (SharePoint) debe de realizarse desde la nube. Esto con el fin que no se generen discrepancias entre contenidos, para garantizar que todas las personas que estén trabajando en un archivo lo estén realizando en tiempo real.
- Asegurar que todas las políticas de seguridad estén en conformidad con las legislaciones de protección de datos aplicables, como el GDPR.
- Aplicar políticas de acceso mínimo necesario, revisando constantemente los privilegios de acceso para asegurar que solo se otorgue a los empleados la información necesaria para sus funciones.
- Establecer directrices claras sobre el uso de redes sociales y navegación en Internet para minimizar los riesgos de seguridad y evitar el uso inapropiado de recursos de la empresa.

Actualización del presente documento

Se debe actualizar por el área de TI de forma periódica o cuando amerite según sea el caso, incluir, aclarar, modificar o retirar una política que afecta la Seguridad de la Información para la Empresa de parques y eventos de Antioquia - ACTIVA**.**

Control de Cambios

Versión	Fecha de Aprobación	Descripción del Cambio
01	26/01/2024	Creación del documento