PLAN TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Aprobó
SANDRA QUIROZ VILLA
Gerente

Elaboró
JUAN DIEGO GIRALDO CHARRY
Coordinador Comunicaciones

ENERO DE 2025

Contenido

INTRODUCCIÓN

La estrategia de Gobierno Digital en Colombia se enmarca en la construcción de un Estado más eficiente, transparente y participativo, que, con el apoyo de las tecnologías de la información y las comunicaciones, refleja un desarrollo sobre la base de los siguientes cuatro ejes temáticos: TIC para el estado, TIC para la sociedad y habilitadores transversales. Atendiendo lo expuesto, el Ministerio de las Tecnologías de la Información y las Comunicaciones, ha definido el Modelo de Seguridad y Privacidad de la Información, denominado MSPI, como un componente transversal basado en la adopción de mejores prácticas y metodologías como: la norma ISO/IEC 27001:2013, entre otras.

Con esta política pública se busca fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública; a través del uso y aprovechamiento de las TI.

Objetivos

El objetivo principal de estas políticas es asegurar la confidencialidad, integridad y disponibilidad de la información del Instituto para el Deporte y la Recreación de Sabaneta INDESA, protegiendo sus activos digitales, recursos y operaciones, cumpliendo con las normativas vigentes y garantizando la continuidad de los servicios. Los objetivos específicos incluyen:

- Proteger la información sensible y confidencial del Instituto contra accesos no autorizados.
- Garantizar la integridad y exactitud de la información y los sistemas de información.
- Asegurar que los sistemas de información estén disponibles para el personal autorizado y los ciudadanos cuando sea necesario.
- Cumplir con todas las normativas y leyes aplicables relacionadas con la protección de la información.
- Fomentar una cultura de seguridad de la información entre el personal y los colaboradores.
- Establecer medidas de prevención, detección y respuesta a incidentes de seguridad

Alcance

Estas políticas se aplican a todos los empleados, contratistas, proveedores y cualquier persona o entidad que maneje información del Instituto para el Deporte y la Recreación de Sabaneta INDESA. Abarca el uso de sistemas, equipos de TI, información almacenada en cualquier medio y sistemas de comunicación que procesan información relacionada con el Instituto.

Clasificación de la Información

Toda la información manejada por el Instituto se clasifica de la siguiente manera:

Pública: Información accesible a cualquier ciudadano sin restricciones.

Confidencial: Información cuyo acceso está limitado al personal autorizado debido a su sensibilidad.

Secreta: Información de alta sensibilidad que podría afectar las operaciones o reputación del Instituto si se divulga sin autorización.

Cada tipo de información debe manejarse con los niveles de seguridad adecuados para su clasificación.

Control de Acceso

- El acceso a la información estará restringido según el rol y las responsabilidades de cada colaborador.

- El personal solo tendrá acceso a la información que necesite para realizar sus funciones.
- El acceso a los sistemas de información estará protegido por contraseñas fuertes.

Uso Aceptable de los Sistemas de Información

- Los sistemas de información del Instituto deben utilizarse únicamente para fines laborales.
- Queda prohibido el uso de los recursos de TI para actividades ilegales o no autorizadas.

- Los usuarios no deben instalar software no autorizado ni modificar la configuración de seguridad de los sistemas.

Gestión de Contraseñas

- Las contraseñas deben cumplir con requisitos mínimos de complejidad: al menos 8 caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales.
- Las contraseñas deben cambiarse cada 90 días.
- Queda prohibido compartir contraseñas entre empleados o con terceros no autorizados.

Protección contra Amenazas

- Todos los sistemas de TI deben estar equipados con software antivirus y soluciones de detección y prevención de intrusiones.
- Se realizarán actualizaciones de seguridad y parches de software de forma periódica para proteger contra vulnerabilidades conocidas.
- Se implementarán cortafuegos para proteger la red interna de accesos no autorizados.

Gestión de Incidentes

- Se establecerá un protocolo de respuesta ante incidentes de seguridad para identificar, gestionar y resolver cualquier brecha de seguridad.
- Cualquier incidente o sospecha de incidente debe ser reportado inmediatamente al equipo de seguridad de la información.
- Se mantendrán registros detallados de todos los incidentes para su análisis y mejora continua.

Backup y Recuperación de Desastres

- Se implementará una política de copias de seguridad periódicas para asegurar la disponibilidad de la información crítica.
- Las copias de seguridad se almacenarán en ubicaciones seguras, tanto locales como externas (almacenamiento en la nube, centros de datos).
- Se realizarán pruebas periódicas de recuperación de datos para garantizar que las copias de seguridad sean funcionales.

Capacitación y Concientización

- Todo el personal debe recibir capacitación anual sobre seguridad de la información, riesgos cibernéticos y las políticas vigentes.
- Se fomentará una cultura de responsabilidad y concienciación en cuanto a la seguridad de la información a través de talleres, seminarios y campañas internas.

Cumplimiento Legal

- Las políticas de seguridad cumplirán con las normativas nacionales e internacionales aplicables, como la Ley de Protección de Datos Personales y las regulaciones locales sobre seguridad de la información.
- Se garantizará que el tratamiento de la información de los ciudadanos y empleados cumpla con los principios de licitud, consentimiento informado y protección adecuada.

Monitoreo y Auditoría

- Se realizará un monitoreo continuo de los sistemas de información para detectar comportamientos sospechosos o no autorizados.

- Se llevarán a cabo auditorías periódicas para asegurar el cumplimiento de estas políticas y evaluar posibles áreas de mejora.

Revisión y Actualización

Estas políticas serán revisadas y actualizadas anualmente o cuando sea necesario debido a cambios en las leyes, normativas o tecnología utilizada por el Instituto.