INSTITUTO MUNICIPAL DEL DEPORTE Y LA RECREACIÓN DE YUMBO

IMDERTY

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

YAMILETH MURCIA

GERENTE

VIGENCIA 2021 – 2023

TABLA DE CONTENIDO

0. INTRODUCCIÓN 3
1. OBJETIVO 4
2. ALCANCE 4
3. MARCO LEGAL 4
4. GLOSARIO 6
5. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 8
6. FASES DE PLANIFICACIÓN 8
6.1 FASE DE EVALUACIÓN DE DESEMPEÑO 11
7. POLITICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN 12
8. RESPONSABILIDADES 19
9. SEGUIMIENTO Y MONITOREO 19

0. INTRODUCCIÓN

La información de la entidad es un activo de gran valor, por lo que los sistemas de información cada vez apoyan más los procesos de misión de la entidad, por lo cual se requiere contar con estrategias eficaces de protección para los datos.

La norma ISO 27001 es un estándar internacional que describe cómo implementar el Sistema de gestión de seguridad de la información de una empresa. Investiga como salvaguardar la información mediante una serie de estándares, lineamientos y procesos que facilitan la identificación de los riesgos. Bajo estos lineamiento El Instituto Municipal del Deporte y la Recreación de Yumbo IMDERTY, reconoce que los sistemas, los activos de información, y la red de información se enfrenta a amenazas de seguridad digital que incluyen, entre muchas otras, fraude, espionaje, sabotaje, vandalismos y desastres naturales.

Las posibilidades de daño y pérdida de datos por causas de código malicioso, poca protección, mal uso de la información, la no definición de procedimientos o ataques, son cada vez más comunes, poniendo en riesgo los activos de información. Por esta razón es importante tener una política que permitan proteger nuestros activos de información y establecer un sistema de gestión y de seguridad de la información.

1. OBJETIVO

Establecer los parámetros necesarios para llevar a cabo los controles necesarios para proteger la información del Instituto Municipal del Deporte y la recreación de Yumbo IMDERTY, como una medida de prevención ante los riesgos y amenazas, buscando evitar la materialización de los mismos, buscando preservar la información.

2. ALCANCE

Esta política aplica a todos los servidores públicos, empleados, contratistas, terceros y partes interesadas del Instituto Municipal del Deporte y la Recreación de Yumbo IMDERTY, que en el ejercicio de las actividades utilicen información y servicios de tecnologías de la información de la entidad.

3. MARCO LEGAL

- Constitución Política. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data; Artículo 20. Libertad de Información.
- Ley 527 de 1999. “Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”
- Ley 962 de 2005. “Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas;”
- Ley 1150 de 2007. “Seguridad de la información electrónica en contratación en línea” • Ley 1266 de 2008. “Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países
- Ley 1273 de 2009. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que

utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Art. 199. Espionaje; Art. 258. Utilización indebida de información; Art. 418. Revelación de Secreto; Art. 419. Utilización de asunto sometido a secreto o reserva; Art. 420. Utilización indebida de información oficial; Artículo 431. Utilización indebida de información obtenida en el ejercicio de la función pública; Artículo 463. Espionaje.

- Ley 1341 de 2009. "Tecnologías de la Información y aplicación de seguridad".
- Ley 1437 de 2011. "Procedimiento Administrativo y aplicación de criterios de seguridad".
- Ley 1581 de 2012. "Por la cual se dictan disposiciones generales para la Protección de Datos Personales".
- Decreto Ley 019 de 2012. "Racionalización de trámites a través de medios electrónicos.
- Ley 1621 de 2013. "Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal y se dictan otras disposiciones".
- Decreto 1078 de 2015, por medio del cual se expide el decreto único reglamentario del sector de Tecnologías de Información y las Comunicaciones
- 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 Tecnologías de la Información y las Comunicaciones"
- Decreto 1413 de 2017. "Por la cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2018, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015 estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- Decreto 415 de 2016. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2011 definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones"
- Política Pública: CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa, CONPES 3854 de 2016 Política Nacional de Seguridad digital. CONPES Bigdata

4. GLOSARIO

Activo: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada Entidad, órgano u organismo.

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO/IEC 27000:2016).

Control: Medida que modifica el riesgo. (NTC ISO 31000:2011). Medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal. (MGRSD 2018).

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una Entidad. (DAFP 2018).

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. (ISO/IEC 27000).

Infraestructura crítica cibernética nacional: Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. (CONPES 3854, pág. 29).

Integridad: Propiedad de exactitud y completitud. (DAFP 2018).

artes interesadas: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad. (MSPI).

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Privacidad: Por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno en Línea la correlativa obligación de proteger dicha información en observancia del marco legal vigente. (MSPI).

Riesgo de 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. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000). POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DANE, INFORMACIÓN PARA TODOS | 12

Seguridad digital: Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (CONPES 3854 2016, pág. 29).

Sistema de Gestión de Seguridad de la Información- SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Vulnerabilidad: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas. (Basado en DAFP 2018)

5. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Instituto Municipal del deporte y la Recreación de Yumbo – Imderty, bajo la política de Gobierno digital donde permite alinearse a los dos componentes: TIC para el Estado y TIC para la Sociedad, se compromete a adoptar las medidas técnicas, jurídicas y administrativas necesarias a través de riesgo, ofreciendo un tratamiento transparente y correcto a la información pública, fomentando una cultura de mejora de la Seguridad de la Información, cuidando los activos de información, para asegurar la confidencialidad, integridad y disponibilidad de la información.

6. FASE DE PLANIFICACIÓN

Para llevar a cabo el desarrollo de esta fase, se procederá a desarrollar el Plan de Seguridad y Privacidad de la Información, alineado con los procesos de la entidad, buscando llevar a cabo los procedimientos de seguridad de la información, roles, responsabilidades, alcance, la política y los objetivos de esta.

Política de seguridad y privacidad de la información. Formular la Política de Seguridad y Privacidad de la información contenida en un documento para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información la cual será divulgada al interior del Instituto Municipal del Deporte y la Recreación de Yumbo - Imderty.

Política Operativas de Seguridad y Privacidad de la Información. Desarrollar un Manual de políticas a nivel operativo, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información para estos se harán capacitaciones al personal del IMDERTY.

Procedimientos de Seguridad de la Información. Desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información. Para desarrollar esta actividad, la Guía No 3 del MSPI- describe los procedimientos mínimos que se deberían tener en cuenta para la gestión de la seguridad al interior del Instituto Municipal del Deporte y la Recreación de Yumbo - Imderty

Roles y Responsabilidades de Seguridad y Privacidad de la Información. El Instituto Municipal del Deporte y la Recreación de Yumbo - Imderty definirá los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativo) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos en el Imderty.

Alta Dirección • Aprobar la política de seguridad y privacidad • Asignar los recursos para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información atendiendo a las necesidades institucionales

Administrador de seguridad de la información • Revisar y validar las políticas generales, complementarias, procedimientos y protocolos en materia de seguridad y privacidad. • Coordinar la implementación de las políticas generales, complementarias, procedimientos y protocolos en materia de seguridad y privacidad. • Evaluar y coordinar la implementación de controles específicos de seguridad y privacidad de la información para los sistemas o servicios del IMDERTY, sean preexistente o nuevos. • Revisar y validar los informes o reportes de actividades en el marco de la Seguridad y Privacidad de la Información para ser presentados a la Alta Dirección.

Proceso gestión jurídica • Asegurar que lo establecido en las políticas generales, complementarias, procedimientos y protocolos den cumplimiento a la normatividad relacionada a la seguridad y privacidad de la información

Inventario de activos de información. Desarrollar una metodología de gestión de activos que le permita generar un inventario de activos de información actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios.

Identificación, Valoración Y Tratamiento de Riesgos. El Instituto Municipal del Deporte y la Recreación de Yumbo – IMDERTY, cuenta con una política de gestión de riesgos la cual debe ser adaptada para que permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos de información, para este periodo se formulará la declaración de aplicabilidad. En esta actividad lo que se desarrollará es una actualización a la política de riesgos para que considere también los riesgos de seguridad de la información y pueda ser usada la metodología ya definida para identificar y valorar los riesgos de seguridad de la información.

Plan de tratamiento de riesgos. La metodología definida en la política de riesgos será aplicada para la identificación, valoración y tratamiento de riesgos de los activos de información relacionados a seguridad de la información una vez tengamos identificados y clasificados todos los activos de información del IMDERTY.

Plan de Capacitación. Definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) del IMDERTY. Este plan será incluido en el Plan Institucional de Capacitación PIC.

Una vez se tengan identificados los riesgos, se identificaran los controles de que mitigarán los riesgos identificados y se procede a realizar el plan de tratamiento de riesgos y la declaración de aplicabilidad.

Adquisición, desarrollo y mantenimiento de sistemas de información Esta política regula la seguridad en los sistemas de información durante todo el ciclo de vida. La Oficina de Sistemas establece una política complementaria para dar lineamientos sobre los criterios necesarios de seguridad de la información para la adquisición, desarrollo y mantenimiento y control de software en los aspectos tales como: (i) uso o instalación de software; (ii) quienes están autorizados para realizar la instalación de software, (iii) cómo se realiza la gestión de solicitudes de instalación de software y (iv) cómo se realiza el inventario de software.

Implementación del plan de tratamiento de riesgos. Desarrollar Informes de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso. Es decir del estado de implementación y efectividad de los controles escogidos para la mitigación de cada riesgo identificado en los activos de información.

Indicadores De Gestión. Definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información.

6.1 FASE DE EVALUACIÓN DE DESEMPEÑO

En esta fase, la oficina de control interno debe desarrollar dentro del proceso de auditorías, debe planificar y desarrollar auditorias para el seguimiento y monitoreo

del MSPI. A continuación se explica de manera general los productos esperados en la fase de Evaluación de desempeño del Modelo de Seguridad y Privacidad de la Información en el Instituto Municipal del Deporte y la Recreación de Yumbo – IMDERTY.

Plan de Ejecución de Auditorias. Se debe llevar a cabo auditorías y revisiones a intervalos planificados que permitan identificar si el MSPI es conforme con los requisitos, está implementado adecuadamente y se mantiene de forma eficaz; así mismo es necesario difundir a las partes interesadas, los resultados de la ejecución de las auditorías y realizar los informes respectivos.

7. POLITICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

- **Seguridad Física del Datacenter.**

La oficina de sistemas tiene restricciones para personal no autorizado, siempre que un usuario desee visitar el Datacenter, este debe estar acompañado por un funcionario responsable del área y por ningún motivo el visitante debe estar solo para garantizar la seguridad física del departamento.

Todas las oficinas deben estar monitoreadas por medio de circuito cerrado de televisión para registrar en medio digital los acontecimientos rutinarios y de excepción.

El administrador o administradores del Datacenter deben garantizar la protección ante desastres con elementos de control de incendios para evitar materializar el riesgo.

Los usuarios de los equipos de cómputo, deben garantizar la confidencialidad de la información, evitando el ingreso de quipos fotográficos, de video, audio u otro equipo que registren información, para evitar comprometer la información confidencial del Imderty.

El administrador del Datacenter debe catalogar el centro de cableado como zona de alto riesgo, con limitación de acceso a personal no autorizado para evitar riesgos físicos en el centro de cableado.

Los usuarios responsables de los equipos, deben evitar el consumo de bebidas y alimentos en los puestos de trabajo, para evitar daños en los equipos de TI.

El administrador del centro de cableado, junto con la alta dirección debe garantizar la seguridad física ante siniestros, evitando que las paredes, pisos y techos contentan material inflamable para evitar incendios u obstaculizar el paso de funcionarios en caso de emergencia.

El administrador de la red de datos debe controlar el ingreso y salida de los recursos de TI en un formato para evitar perdida de los elementos de TI de propiedad del IMDERTY.

Seguridad de la Red de Datos

El administrador de la red de datos debe garantizar que la conectividad a los servicios de la red deben llevarse a cabo con al menos un método autenticación que incluya usuario y contraseña para evitar y controlar los usuarios que acceden a los servicios de TI.

Seguridad en las Operaciones

El administrador de la red datos, debe garantizar la detección de códigos maliciosos, por el cual todos los equipos deben contar con programas antivirus instalados y están en operación para que permita eliminar cualquier virus de este y/o de otros medios.

El administrador de la red de datos, debe garantizar que los software que tengan instalados los equipos deben ser actualizados cada que el fabricante del software libere una actualización para evitar parar los procesos de la entidad.

El administrador de la red, debe instalar un Firewall de software en los equipos de cómputo de manera manual o automática, para monitorear, proteger y controlar los puertos lógicos del equipo de cómputo.

El administrador de la red de datos, debe garantizar que los diferentes medios extraíbles que los usuarios conecten a los equipos deberán ser explorados por el software antivirus que se encuentra instalado para protegerlos contra códigos maliciosos.

El administrador de la red de datos, es la única persona autorizada para la instalación de software para evitar que se instalen software sin licenciamiento o que se atente con la integridad de la red del IMDERTY.

Los usuarios de los equipos de cómputo deben bloquear la pantalla cuando se levanten del puesto por largo tiempo para evitar accesos no autorizados a los equipos de cómputo.

Los usuarios de los equipos de cómputo son responsables de apagar los equipos que usan para sus labores diarias cada que termine su jornada laboral para evitar que estos sean utilizados para otro fin.

El administrador de la red de datos debe garantizar que el antivirus cuente con soporte técnico, y servicios de alerta. Administrando y monitoreando la consola de antivirus para mantener controlados los riesgos de código malicioso en la red de la administración central.

Los usuarios y funcionarios del IMDERTY, que cuenten con correo electrónico institucional, deben preservar la seguridad de su correo manteniendo la privacidad, confidencialidad de la información de acceso y la información contenida en él, para evitar suplantación y fuga de información.

El administrador de datos, debe garantizar la realización de copias de seguridad (Backups), donde se verifique su realización, almacenamiento y pruebas de integridad para mantener puntos y tiempos objetivos de recuperación adecuados.

El responsable de la red de datos debe probar los backup realizados con regularidad para confirmar de que se puede hacer una restauración completa.

El responsable de los backups debe documentar la forma en la que se hacen los respaldos de información.

El encargado de las copias de respaldo debe asegurar que las copias se realicen de manera automática por medio de un programa de copia y se debe configurar según solicitud realizada en el procedimiento para garantizar la realización de las copias de respaldo.

Políticas para el control de acceso

El administrador de la red de datos, debe asignar un usuario único y exclusivo a los funcionarios y contratistas que ejercen funciones públicas cuyos privilegios de acceso a los equipos de cómputo estarán determinados por el tiempo de vinculación con la entidad y asi de esta manera poder mantener el control a los equipos.

A los funcionarios y contratistas que ingresen a la entidad por primera, se les debe asignar una nueva clave de acceso con el fin de mantener la privacidad de la información.

Los funcionarios y contratistas deben asegurarse que los usuarios y contraseñas no deben ser compartidos con el fin de mantener la privacidad de la información.

Los funcionarios y contratistas que ejercen sus funciones públicas deben solicitar al administrador de la red de datos, el cambio de su contraseña cada 60 días y esta no puede coincidir con las 5 anteriores.

Política para la adquisición, desarrollo y mantenimiento de sistemas de información

El administrador de la red de datos, debe asegurar que para todos los sistemas de información debe ser auditada en cuanto a capacidad y seguridad utilizando las mejores metodologías para mantener características mínimas de seguridad alineadas a estándares de seguridad.

El responsable de la red de datos, debe asegurar la definición de roles, permisos y control de acceso a las aplicaciones y las carpetas del sistema de información.

El responsable de la red de datos debe definir, documentar e informar a la subgerencia administrativa del Imderty los permisos exactos de los usuarios del sistema operativo de acuerdo a la estricta necesidad de operación del sistema de información desarrollado para mantener el debido control de acceso a los sistemas.

El responsable de la red de datos debe asegurar que la carga de archivos y la parametrización del sistema de información debe realizarse únicamente desde direcciones IP aprobadas por el Imderty para disminuir el riesgo de instrucción desde redes externas.

8. RESPONSABILIDADES

La Alta dirección del Imderty, es la responsable de la coordinación, seguimiento y verificación de la implementación y desarrollo de la estrategia de Gobierno en Línea.

El área de Control Interno junto con el comité de Gestión y Desempeño, son los responsables de la aprobación de la Política de Seguridad de la Información en el Instituto Municipal del Deporte y la Recreación de Yumbo – Imderty.

El líder de Ti, elaborará el mapa de riesgos de Seguridad de la Información y este será aprobado por la alta dirección del Imderty.

La oficina de comunicaciones será la encargada de la publicación de la Política de la Información.

El área de Talento Humano articulado con el área de Sistemas del Imderty, serán los encargados de promover el uso y apropiación de la Política de Seguridad de la Información.

El área de Calidad, será la encargada de codificar la Política de Seguridad de la Información.

9. SEGUMIENTO Y MONITOREO

El comité de Gestión y Desempeño, articulado con la Oficina de Control Interno y el Área de Sistemas realizarán el monitoreo de la Política de la Seguridad de la Información por lo menos una vez al año.

Los líderes de los procesos harán revisión de los controles establecidos según la periocidad definida en el plan de tratamiento de riesgos de información definida por la entidad.