INSTITUTO DEPARTAMENTAL DE RECREACIÓN Y DEPORTES INDERSANTANDER

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONTENIDO

DEFINICIONES

Aceptación del riesgo: Decisión de asumir un riesgo.

Activo: Es todo aquello que tiene valor para la organización (Información, Software, Hardware, Servicios, Imagen institucional, Personas) y necesite protegerse.

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

Análisis de riesgo: Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

Autenticidad: Permite verificar la identidad del generador de la información, evitando la suplantación de identidad.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Contraseña: Conjunto de números, letras y caracteres, utilizados para reservar el acceso a los usuarios que disponen de esta contraseña.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Evento de seguridad de la información: Es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Gestión documental: Conjunto de actividades administrativas y técnicas tendientes a la planificación, manejo y organización de la documentación producida y recibida por las entidades, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación.

Gestión de Incidentes: Conjunto de acciones y procesos tendientes a brindar a las organizaciones fortalezas y capacidades para responder en forma adecuada a la ocurrencia de incidentes de seguridad informática que afecten real o potencialmente sus servicios.

Inalterabilidad: Garantizar que un documento electrónico generado por primera vez en su forma definitiva no sea modificado a lo largo de todo su ciclo de vida, desde su producción hasta su conservación temporal o definitiva.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una

probabilidad significativa de comprometer las operaciones del negocio y amenazar a seguridad de la información.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de la información.

Medios de almacenamiento removibles: comprende los discos duros externos, memorias USB, tarjetas SD, etc.

No repudio: el emisor no podrá negar el conocimiento de un mensaje de datos ni los compromisos adquiridos a partir de éste.

Política: Toda intención y directriz expresada formalmente por la Alcaldesa Municipal.

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.

Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

Sistema de gestión de la seguridad de la información - SGSI: Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar. Hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

Recursos TIC: Las Tecnologías de la información y la comunicación - TIC, comprende la red local, internet, página web, correo electrónico, sistemas de información, carpetas compartidas y demás recursos tecnológicos de apoyo al logro de los objetivos de la Administración Municipal.

Usuario: Toda persona que utilice los sistemas de información de la entidad debidamente identificado y autorizado a emplear las diferentes aplicaciones habilitadas de acuerdo con sus funciones.

Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

INTRODUCCIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, mediante el artículo 7 de la Resolución 4870 de 2023, - "Por la cual se establecen el Modelo Integrado de Gestión (MIG) y el Sistema Integrado de Gestión (SIG) del Ministerio de Tecnologías de la Información y las Comunicaciones/Fondo Único de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 2175 de 2022 y sus modificatorias.", definió la relevancia de integrar los modelos y sistemas de gestión de la entidad de manera articulada con el Modelo Integrado de Gestión en los siguientes términos:

"[…] La instauración de otros sistemas de gestión en la Entidad deberá ser presentada al Comité MIG para su aprobación por parte del Líder del Sistema que se requiere adoptar. La Oficina Asesora de Planeación y Estudios Sectoriales del MinTIC, deberá gestionar la alineación correspondiente a los sistemas de gestión y modelos que se requieran normativamente, así como los que se desarrollen por iniciativa de la Entidad".

Así mismo, indica que debe para la sostenibilidad y mejoramiento continuo del Modelo Integrado de Planeación y Gestión se establece la necesidad de cumplir con la Política de Gobierno Digital, en relación de las políticas de Gestión y Desempeño Institucional MIPG, de acuerdo con las cuales los Líderes de los diferentes Sistemas de Gestión y el Comité MIG son responsables de planear y ejecutar las acciones necesarias para la implementación de los requisitos de cada política, bajo el acompañamiento y seguimiento de la Oficina Asesora de Planeación y Estudios Sectoriales de MinTIC

En el mismo sentido, el Decreto 2106 de 2019, "por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública", indica en su artículo 16 que "[l]as autoridades que realicen trámites, procesos y procedimientos por medios digitales deberán disponer de sistemas de gestión documental electrónica y de archivo digital, asegurando la conformación de expedientes electrónicos con características de integridad, disponibilidad y autenticidad de la información", por lo que es menester disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital y está determinada por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de esta, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.[1]

[1] Ministerio de Tecnologías de La información y las Comunicaciones –MinTIC- tomado: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mintic.gov.co/portal/715/articles-135830_plan_seguridad_privacidad_informacion_2024_20240125.pdf

1.OBJETIVOS

1.1. OBJETIVO GENERAL

Establecer las actividades contempladas en el Modelo de Seguridad y Privacidad de la Información – MSPI de la política de Gobierno Digital del MinTIC, alineadas con la NTC/IEC ISO 27001 la Política pública de Seguridad Digital, y los criterios de Continuidad de la operación de los servicios, que permitan mantener la seguridad y privacidad de la información que circula en los procesos del Ministerio/ Fondo Único de TIC.

1.2. OBJETIVOS ESPECÍFICOS

- Proteger los activos de información de la Administración Municipal, con base en los criterios de confidencialidad, integridad y disponibilidad.
- Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.
- Sensibilizar a los servidores públicos y contratistas de la Entidad acerca del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información críticos de la Entidad.
- Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico.
- Implementar acciones correctivas y de mejora para el Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información de la Política de Gobierno Digital.

2.RESPONSABILIDADES

1. Aprobar los lineamientos, metodologías relacionadas con la seguridad de información y Gobierno Digital.
2. Coordinar la implementación de los modelos de Gobierno Digital y de seguridad de la información.
3. Revisar el avance en la implementación de los modelos de Gobierno Digital y de seguridad de información.
4. Aprobar lineamientos, metodologías y practicas al interior de la Administración Municipal para la implementación de las estrategias demarcadas en los modelos descritos.
5. Diseñar las estrategias para la apropiación de los modelos de Gobierno Digital y de seguridad de la información.

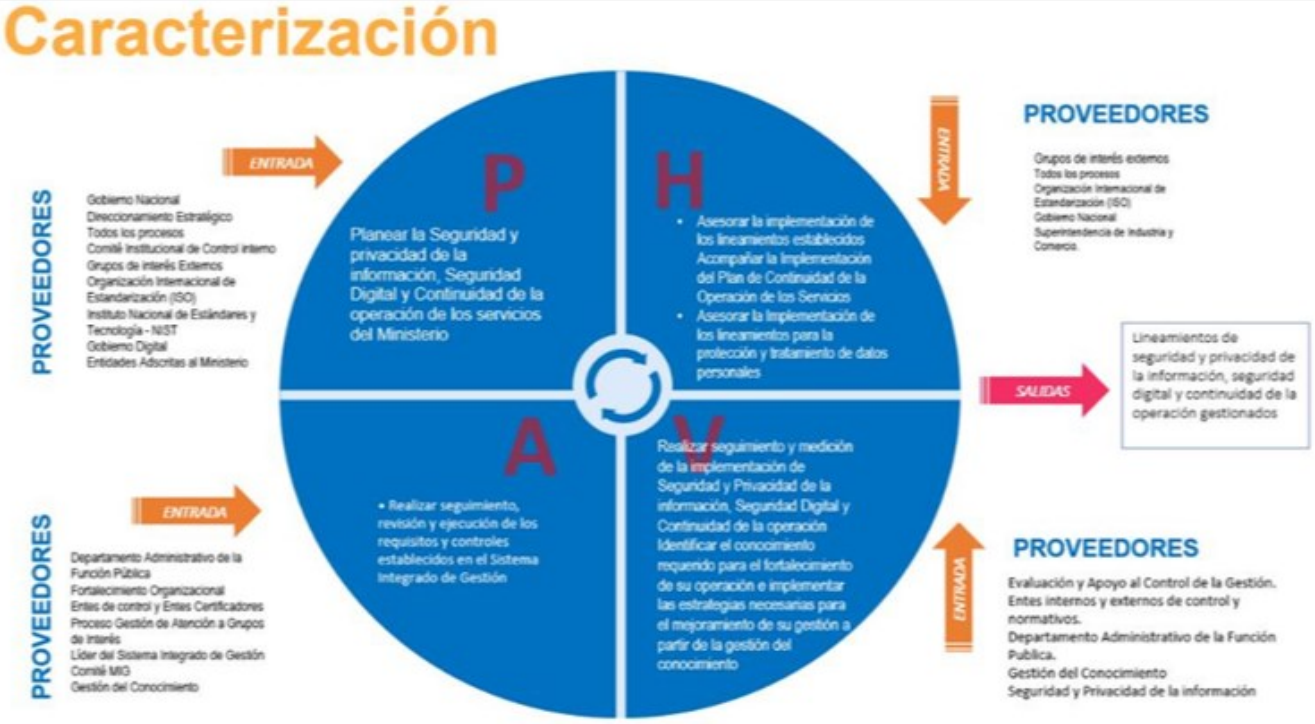
Por lo anterior, se deben tener en cuenta al responsable de Tecnologías de la Información y Seguridad Digital de la Administración en las reuniones del Comité Institucional de Gestión y Desempeño.

De la misma manera y en el entendido que el sistema de Seguridad de Información no es un sistema aislado, todos los funcionarios, contratistas y partes interesadas son parte activa del desarrollo e implementación del MSPI, teniendo claridad que son ellos, los propietarios de activos de información y el frente de vulnerabilidades más atacado por las amenazas.

3. PROCESO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

MODELO PHVA

El Sistema de Gestión de la Seguridad de la Información –SGSI- inmerso dentro del MSPI, se basa en la necesidad que la seguridad de la información esté en continua evolución y que, además, dicha evolución esté documentada y justificada. El modelo en el que se basa el SGSI es denominado PHVA (Planear-Hacer-Verificar- Actuar).



Ciclo PHVA del proceso de Seguridad y Privacidad de la Información

Fuente; Mintic

4. PLANEAR

En esta primera fase se realiza un estudio de la situación actual del Instituto Departamental De Recreación Y Deportes Santander, desde el punto de vista de la seguridad de la información, es necesario estimar las medidas que se van a implementar en función de las necesidades detectadas, determinando así el alcance del MSPI y la Política de Seguridad.

Se debe tener en cuenta que no toda la información del Instituto Departamental De Recreación Y Deportes Santander tiene el mismo valor en cuanto a los tres pilares (confidencialidad, integridad y disponibilidad), e igualmente, no toda la información está sometida a los mismos riesgos. Por ello, una de las actividades importantes dentro de esta fase es la realización de la gestión de riesgos que ofrezca una valoración de los activos de información y las vulnerabilidades a las que están expuestos, así como también, evaluar los posibles impactos para la Entidad y con base en ello, establecer planes de acción con miras a minimizar dichos riesgos, lo anterior se realiza tomando como base el registro de activos

de información de la Entidad el cual permite identificar los activos de mayor criticidad. Las actividades por realizar para obtener un inventario de activos serán:

1. Se realizará la gestión de activos de información por medio del formato elaborado para este fin, se tendrá en cuenta los activos de información de carácter documental, hardware y software.

2. Definir las responsabilidades y roles de los activos de información con los líderes de los procesos.

3. Verificar si un activo de información continua o no siendo parte del inventario, o si los valores de evaluación asignados en el inventario y clasificación de activos de Información deben ser modificados.

4. Actualizar el inventario de activos con una periodicidad de seis meses

5. Publicar en la página web el registro de activos de información, para esta acción y por tratarse de un documento confidencial, según lo define el MinTic, es necesario formular una versión publica la cual no contenga datos como nombres de servidores, direcciones IP, nombres de Sistemas de Información, etc.

4.1. Contexto de la Entidad

Consiste en conocer el Instituto Departamental De Recreación Y Deportes de Santander como una entidad que presta servicios y tramites a sus usuarios en marco de su Misión, apoyada de su estructura organizacional, sistemas de información y procesos institucionales con el objetivo de cumplir lo establecido en su Visión.

También se debe identificar las necesidades del Indersantander y sus usuarios relacionada con la seguridad de la información partiendo desde los requerimientos realizados por los usuarios durante la solicitud de trámites.

Para ello es importante comprender los procesos y procedimientos en los que se soporta para cumplir sus objetivos, mirar el contexto interno y externo de la Entidad, definir los flujos de información con cada una de las partes interesadas y en general, comprender a la entidad como un Sistema, dando como resultado

el entendimiento de la Entidad y a partir de eso, la definición del alcance del Sistema de Seguridad de Información, los objetivos del MSPI y la Política general de seguridad de la información.

4.2.Alcance del SGSI - MSPI

EL SGSI- MSPI es aplicable a los activos de información de todos los procesos de la Entidad, verificándolo y aplicándolo en cada área, y comprende las políticas, procesos, procedimientos y controles para la preservación de confidencialidad, integridad y disponibilidad de la información.

4.3. Objetivo General del SGSI - MSPI

Definir e implementar directrices y lineamientos necesarios para fortalecer la seguridad de la información y garantizar la disponibilidad, integridad y confidencialidad de la misma dentro de la Entidad.

4.4. Objetivos Específicos del SGSI - MSPI

1. Definir controles y políticas para proteger la información de la Entidad frente a los criterios de confidencialidad, integridad y disponibilidad.

2. Implementar la metodología de Administración y Gestión de Riesgos con el fin de disminuir el impacto en una posible materialización de un riesgo.

3. Fortalecer el nivel de conciencia de los funcionarios y contratistas del Instituto Departamental De Recreación Y Deportes de Santander en cuanto a la seguridad de los activos y de la información por medio de capacitaciones.

4. Monitorear el cumplimiento de los controles de seguridad de la información.

5. Definir los procesos para mejora continua del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información.

4.5. Políticas de Seguridad de la Información

La definición de los siguientes controles administrativos y operacionales están diseñados a regular de manera efectiva el acceso de usuarios a nivel de aplicación, sistema operativo, bases de datos, red y acceso físico.

4.5.1. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Indersantander reconoce la información como un activo fundamental para la prestación de los servicios y la toma de decisiones, por lo cual declara su compromiso con la preservación de la confidencialidad, integridad y disponibilidad de sus activos de información, la planeación, implementación, operación y mejora continua del sistema de gestión de seguridad de la información - SGSI en el marco de la norma NTC ISO/IEC 27001, soportada en los objetivos de la Administración Municipal y los lineamientos nacionales y regulatorios.

Las presentes políticas de seguridad de la información deberán permanecer actualizadas y publicadas para el acceso y conocimiento de todos los usuarios del Indersantander.

4.5.2. POLÍTICAS DE SEGURIDAD DEL PERSONAL

Todo usuario de bienes y servicios informáticos al ingresar como funcionario o contratista acepta las condiciones de confidencialidad, de uso adecuado de los recursos informáticos y de información del Instituto Departamental De Recreación Y Deportes de Santander, así como el estricto cumplimiento de las Políticas de seguridad mencionadas en este documento.

Revisión de Antecedentes antes de la Contratación

Toda vez que se requiera vinculación de personal de planta o contratistas, se debe realizar una revisión de los antecedentes de acuerdo con los requisitos del cargo y el tipo de información a la cual tendrá acceso.

Usuario Nuevo

Todo personal nuevo del Instituto Departamental De Recreación Y Deportes de Santander, deberá ser notificado por cada Secretario o Supervisor del contrato al Líder de Tecnología del INDERSANTANDER con el fin de ser creado como usuario de las bases de datos correspondientes, asignar los servicios TIC

(internet, correo electrónico, etc.) requeridos para el correcto desempeño de funciones y/o actividades.

***NOTA**: Se deberá generar un formato de registro y solicitud de servicios de TIC para la gestión de usuarios, este deberá ser aprobado por el Comité Institucional de Gestión y Desempeño.*

Acuerdo de Confidencialidad

- Dentro de los contratos de proveedores se deben incluir las cláusulas de confidencialidad de la información.
- Los supervisores de contratos y jefes inmediatos son responsables de velar por el cumplimiento de las cláusulas de confidencialidad.
- Los Funcionarios de la Entidad deben firmar el formato “Acuerdo de Confidencialidad” (Ver anexo 1: Acuerdo de Confidencialidad) en el momento de su vinculación al Instituto Departamental De Recreación Y Deportes Indersantander.

Confidencialidad Personal Contratista

Cualquier información intercambiada, facilitada o creada entre el contratista y el Instituto Departamental De Recreación Y Deportes de Santander en el transcurso de su vinculación, será mantenida en estricta confidencialidad. La parte receptora correspondiente sólo podrá revelar información confidencial a quienes la necesiten y estén autorizados previamente por la parte titular de la información confidencial. Se considera también información confidencial:

1. Aquella que haya sido declarada como confidencial por el responsable o propietario de la información,

2. La que no sea de fácil acceso,

3. Aquella información que esté sujeta a medidas de protección razonables, de acuerdo con las circunstancias del caso, a fin de mantener su carácter confidencial.

4. Aquella que por su naturaleza sea considerada como confidencial. No habrá deber alguno de confidencialidad en los siguientes casos: **a)** Cuando la parte receptora tenga evidencia de que conoce previamente la

información recibida; **b)** Cuando la información recibida sea de dominio público y, **c)** Cuando la información deje de ser confidencial por ser revelada por el propietario. El presente acuerdo tendrá una duración indefinida y terminará cuando las partes de común acuerdo lo determinen.

Entrenamiento en Seguridad Informática

- Todos los funcionarios nuevos deberán ser informados sobre las Políticas de Seguridad de la Información en la capacitación de inducción.

- Todos los funcionarios y contratistas deben recibir entrenamiento y toma de conciencia en seguridad de la información.

Terminación Laboral

- Todo funcionario o contratista que se desvincula al Instituto Departamental De Recreación Y Deportes de Santander debe realizar la devolución de los activos de información a su cargo y el Líder de Tecnología deberá certificar su paz y salvo, lo anterior con el fin de deshabilitar cuentas de correo, usuarios de acceso a las aplicaciones, entrega de información gestionada durante la ejecución contractual.

- Todo funcionario o contratista que se desvincula del Indersantander debe entregar a su jefe inmediato o supervisor de contrato la copia de respaldo de los documentos que soportan el cumplimiento de sus funciones en caso de funcionarios o la ejecución de los alcances del contrato en caso de contratista.

Medidas Disciplinarias

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de la del Instituto Departamental De Recreación Y Deportes de Santander, o las contempladas en la Ley 1273 de 2009. En caso de presentarse violación a las políticas de seguridad de la información se debe informar a la oficina de Control Interno para los fines correspondientes.

4.5.3. POLÍTICA DE GESTIÓN DE ACTIVOS

Todos los activos de información del Indersantander deben estar debidamente identificados incluyendo el responsable, su ubicación, criticidad (valorado según la confidencialidad, integridad y disponibilidad) y clasificación.

Clasificación de la Información

Con el fin de asegurar que la información recibe el nivel apropiado de protección, de acuerdo con su importancia para la Entidad, se ha adoptado la siguiente clasificación para toda la información que genere del Instituto Departamental De Recreación Y Deportes de Santander en desarrollo de sus objetivos:

Pública: Es toda información que la Entidad genere, obtenga, adquiera, o controle que ha sido declarada, legalmente o por su propietario de conocimiento público y accesible a cualquier persona. *Ejemplo*: Plan de Desarrollo Municipal, datos abiertos, etc.

Uso interno: Información que es utilizada y generada por el personal de la Entidad en cumplimiento de sus labores, y que sin ser confidencial ni reservada no es publicada para conocimiento de terceros, sin embargo, podrá ser conocida mediante solicitud a la Entidad. *Ejemplo:* Memorandos, correos, reportes para entidades, manuales, documentos de trabajo.

Confidencial: Información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto financiero, potencial de fraude o requisitos legales. Solo puede ser vista por un grupo de personas o un área en particular. La divulgación a terceros solo se hace bajo autorización de un nivel directivo o autoridad competente. *Ejemplo*: Configuración de equipos, resultados de evaluación de riesgos de seguridad de la información, procesos disciplinarios, etc.

Reservada: Es aquella información que estando en poder o custodia de la Entidad, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014.

Los propietarios o responsables de la información deben clasificar cada uno de los documentos o información generada en el ejercicio de sus funciones.

Entiéndase como propietario o responsable de la información al funcionario o cargo que tiene la responsabilidad de definir quienes tienen acceso y que pueden hacer con la información y de determinar cuáles son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada y al mismo tiempo de definir que se hace con la información una vez ya no sea requerida y los tiempos de retención asociados a la misma.

Uso Aceptable de los Activos

Es deber de todos los funcionarios y contratistas del Instituto Departamental De Recreación Y Deportes de Santander hacer uso adecuado y responsable de los activos de información a su cargo preservando la confidencialidad, integridad y disponibilidad de los mismos.

Los recursos TIC dispuestos por el Instituto Departamental De Recreación Y Deportes de Santander es el para el uso por parte de los Funcionarios y Contratistas autorizados deben emplearse sólo con fines laborales.

Prohibiciones en el uso de los Activos de Información

- Incluir en correos electrónicos, documentos, imágenes, boletines, redes sociales institucionales u otras formas de comunicación, contenido que razonablemente puede considerarse una amenaza, acoso, u ofensa para cualquier persona, o que viole la política colombiana sobre acoso laboral y abuso de autoridad.

- Ofrecer acceso a los recursos de las TIC o poner a disposición de personas datos sin autorización previa para acceder a ellos.

- Alterar, ocultar, suprimir o compartir datos sin autorización.

- Uso de redes de intercambio de archivos (Ares, BitTorrent, Spotify, aTube cátcher) a fin de obtener ilegalmente material con derechos de autor y la instalación de software que no ha sido aprobado para su uso.

- Acceder a internet a visualizar, compartir y descargar material pornográfico, videos, música, películas o escuchar emisoras online.

- Copia no autorizada de material protegido por derechos de autor propiedad del Instituto Departamental De Recreación Y Deportes de Santander.

- Generar o enviar correos electrónicos a nombre de otro usuario sin autorización o suplantándolo.

- Burlar los mecanismos de seguridad, autenticación, autorización o de auditoría, de cualquier servicio de red, aplicación, servidor o cuenta de usuario.

Uso del Correo Electrónico Institucional

- Toda comunicación por correo electrónico de origen laboral debe ser tramitada desde el correo institucional, está prohibida la utilización del correo personal para los fines laborales.

- Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe re direccionar el correo a otra cuenta de correo interno.

- Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad del Instituto Departamental De Recreación Y Deportes de Santander.

- Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.

- Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

- Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas del Instituto Departamental De Recreación Y Deportes de Santander.

- La cuenta de correo institucional no debe ser inscrita en páginas o sitios publicitarios ajenos a los fines laborales.

Administración y Uso de Contraseña

- La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.
- Cuando un usuario olvide o bloquee su contraseña, deberá acudir personalmente al Líder de Tecnología para que se le proporcione una nueva contraseña.
- Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y/o lógico y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.
- Se deben seguir las siguientes recomendaciones con el fin de evitar la utilización de contraseñas débiles:
- Evitar utilizar la misma contraseña siempre en todas las aplicaciones.
- Evitar utilizar secuencias básicas de teclado (por ejemplo: “qwerty”, “asdf” o en numeración: “1234” ó “98765”
- No repetir los mismos caracteres en la misma contraseña. (ej.: “111222”)
- No utilizar como contraseña las fechas especiales, número de identificación ni nombre de seres queridos.
- Evitar también utilizar solamente números, letras mayúsculas o minúsculas en la contraseña.
- No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña
- Las contraseñas deben tener una longitud mínima de 8 caracteres y estar compuesta por tres de las siguientes características con el fin de crear contraseñas robustas, difíciles de descifrar:
- Utilizar números.
- Utilizar letras Mayúsculas.
- Utilizar letras Minúsculas.
- Incluir algún carácter especial (@$%/#_-.).
- Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, deberá cambiarla inmediatamente.

Control de Accesos Remotos

La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y el Líder de Tecnología.

Resguardo y Protección de la Información

- El usuario deberá reportar de forma inmediata al Líder de Tecnologías de del Instituto Departamental De Recreación Y Deportes de Santander, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

- El usuario tiene la obligación de proteger las unidades de almacenamiento que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.

- Es responsabilidad del usuario evitar en todo momento la fuga de la información del Instituto Departamental De Recreación Y Deportes de Santander que se encuentre almacenada en los equipos de cómputo que tenga asignados.

Protección y Ubicación de los Equipos

- Los usuarios no deben mover, reubicar o abrir los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del Líder de Tecnología, en caso de requerir este servicio deberá solicitarlo.

- El equipo de cómputo asignado a funcionarios o contratistas, deberá ser para uso exclusivo de las funciones del Instituto Departamental De Recreación Y Deportes de Santander.

- Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

- Mientras se opera cerca del equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

- Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o de la torre.

- Se debe mantener el equipo informático en un entorno limpio y sin humedad.

- El usuario debe asegurarse que los cables de conexión no sean pisados o trozados al colocar otros objetos encima o contra ellos, en caso de que no se cumpla solicitar un reacomodo de cables con el personal autorizado.

- Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser realizados por el personal autorizado.

Mantenimiento de Equipo

- Únicamente el personal autorizado podrá llevar a cabo el mantenimiento preventivo y/o correctivo de los equipos informáticos.

- Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

Pérdida de Equipo

- El usuario que tenga bajo su resguardo algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien en los casos de robo, extravío o pérdida del mismo.

- El usuario deberá dar aviso inmediato al Líder de Tecnología y almacén de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

Uso de Dispositivos Especiales

- El uso de los grabadores de discos compactos (unidades de cd/dvd) es exclusivo para copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.

- El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

Daño del Equipo

Se levantará un reporte de incumplimiento de las políticas de seguridad contra el usuario que provoque algún daño por maltrato, descuido o negligencia a un equipo de cómputo o cualquier recurso de tecnología de información.

Baja de los Equipos

El responsable del estado de los equipos de cómputo del Instituto Departamental De Recreación Y Deportes de Santander debe emitir concepto técnico de cada uno de los equipos susceptibles a dar de baja, determinando el estado del activo con el fin de establecer su destino final.

Se debe realizar una primera destrucción de los medios de almacenamiento de información antes de ser entregado a la empresa de disposición de residuos electrónicos.

Uso de Medios de Almacenamiento

Todos los medios utilizados para almacenamiento de las copias de respaldo o para almacenamiento de información en tránsito deben permanecer resguardados de forma segura evitando su acceso por parte de personas no autorizadas.

Registros de Eventos

Las actividades que realicen los usuarios en la infraestructura de Tecnología de Información de la Administración Municipal deben ser registradas y protegidas contra alteración y acceso no autorizado, los cuales se deben revisar regularmente con el fin de detectar violaciones a la seguridad de la información.

Gestión de Cambios y Capacidad

Los cambios realizados a los sistemas de información deben ser controlados, para lo cual se debe solicitar el cambio al Líder de Tecnología.

Para cada cambio o adquisición de recursos TIC se deben identificar los requisitos de capacidad necesarios con el fin de adaptar el sistema para garantizar su eficacia.

Seguridad con Proveedores

Se deben establecer, acordar y documentar los requisitos de seguridad con los proveedores con el fin de mitigar los riesgos asociados con el acceso de proveedores a los activos de la Corporación.

Identificación del Incidente

El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el usuario informático lo deberá notificar al Líder de Tecnologías.

Administración de la Configuración

Los usuarios del Instituto Departamental De Recreación Y Deportes de Santander no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP, SSH), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la Entidad.

Seguridad para la Red

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada, en la cual los usuarios realicen la exploración de los recursos informáticos en la red, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

Controles contra Código Malicioso-VIRUS

Para prevenir infecciones por virus informático, los usuarios de la Administración Municipal no deben hacer uso de software que no haya sido proporcionado y validado.

Los usuarios deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado e instalado.

Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y reportar el incidente para la detección y erradicación del virus.

Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implementadas.

Uso de Redes Sociales

No está permitido el uso de redes sociales y mensajería instantánea desde los equipos de cómputo de la Administración Municipal por razones de seguridad, los usuarios que requieran acceso a estos servicios deberán realizar la solicitud debidamente justificada.

Internet

- El acceso a internet provisto a los usuarios es exclusivamente para las actividades relacionadas con las necesidades de las funciones y/o objeto contractual que desempeña.
- Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por la Administración Municipal, en caso de necesitar una conexión especial a Internet, ésta tiene que ser notificada.
- Los usuarios del servicio de navegación en Internet, al usar el servicio están aceptando que:
    - Serán sujetos de monitoreo de las actividades que realiza en Internet.
    - Saben que existe la prohibición al acceso de páginas no autorizadas.
    - Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.

- Saben que existe la prohibición de descarga de software sin autorización.
- Saben que el tráfico de la red esta priorizado en función de su contenido evitando el mal uso de la herramienta y la congestión en la misma por el hecho de bajar películas, videojuegos, jugar en línea y el uso de audio y video Real player que consume recursos de red provocando pérdidas de conexión.
- La utilización de Internet es para el desempeño de su función y/o objeto contractual y no para propósitos personales.

Derechos de Propiedad Intelectual

Todo material desarrollado por funcionarios o contratistas en desarrollo de sus funciones o la ejecución de los alcances del contrato, en horario laboral y con la información suministrada por el Instituto Departamental de Recreación y Deportes de Santander son propiedad del Indersantander.

4.5.4. Identificación y Clasificación de Activos de Información

Un activo de información, según la ley 1712 de 2014, es el elemento de información que el Indersantader recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita, en papel, trasmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes.

Para la identificación de los activos de información es necesario conocer los procesos y subprocesos que están dentro del alcance del SGSI-MSPI, ya que estos procesos y subprocesos serán los responsables de dichos activos y por lo tanto quienes suministren la información, valoración, ubicación y clasificación de los mismos. (Ver anexo 2: Registro de Activos de Información).

Análisis de Brecha

El análisis de brecha busca generar un diagnóstico relativo a la seguridad de la información basado en la identificación de diferencias entre el estado actual y el estado ideal del Instituto Departamental De Recreación Y Deportes de Santander de acuerdo con los requerimientos exigidos en la norma ISO 27001:2013, el modelo de seguridad y privacidad de la Información - MSPI y las consideraciones definidas internamente como parte del ejercicio de la Entidad y el cumplimiento de su Misión.

Las fases para realizar una metodología de diagnóstico de seguridad de la información son:

- Revisión del cumplimiento de las exigencias de la Norma ISO 27001 en concordancia con el modelo de seguridad y privacidad de la Información - MSPI, respecto a la Seguridad de la Información, la gestión de los riesgos, el análisis de vulnerabilidades y el seguimiento a las mismas.

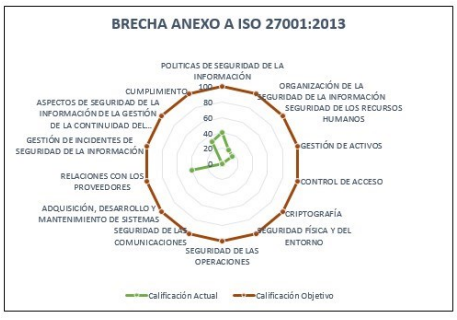
- Revisión de los controles existentes que apliquen a la seguridad de la información en la Administración Municipal según el anexo A de la citada Norma.

- Identificar requisitos faltantes (Políticas, procedimientos, controles), los cuales son exigidos por la norma ISO 27001 y por los modelos del MinTic – MSPI.

En cumplimiento con lo establecido por el MinTic, se va a usar la herramienta de diagnóstico de seguridad y privacidad de la información (Anexo 3), la cual arroja un resultado que permite a cada entidad visualizar los diferentes dominios de la norma, evaluar las falencias y a partir de eso, generar un plan de seguridad de la información para ser desarrollado al interior de la misma y dar cumplimiento con lo estipulado en el manual de gobierno digital en sus diferentes componentes. Como resultado de este diagnóstico se obtiene lo siguiente:

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	40	100	REPETIBLE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	16	100	INICIAL
A.8	GESTIÓN DE ACTIVOS	0	100	INEXISTENTE
A.9	CONTROL DE ACCESO	0	100	INEXISTENTE
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	0	100	INEXISTENTE
A.12	SEGURIDAD DE LAS OPERACIONES	0	100	INEXISTENTE
A.13	SEGURIDAD DE LAS COMUNICACIONES	0	100	INEXISTENTE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	100	INEXISTENTE
A.15	RELACIONES CON LOS PROVEEDORES	40	100	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	100	INEXISTENTE
A.18	CUMPLIMIENTO	31	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		11	100	INICIAL



Documentación de Procedimientos

Durante esta fase se identificarán y documentarán procedimientos necesarios para dar cumplimiento a la norma ISO 27001 y a las necesidades propias que la Entidad requiere, garantizando un adecuado funcionamiento del Sistema de

Gestión de Seguridad de la Información - MSPI. La Administración Municipal deberá formular los siguientes procedimientos:

Administración de Gestión de Usuarios
Mantenimiento y soporte
Administración Servidores
Administración de Hardware
Administración Software
Administración de Antivirus
Generación de Backups en servidores
Generación de Backups de Equipos de Cómputo
Registro y solicitud de servicios de TIC

4.5.5. Metodología para la Gestión de Riesgos

La gestión de riesgos de seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento, el cual es adoptado como Política de Seguridad Digital la cual contiene la metodología de Gestión de riesgos basada en el Modelo de Riesgos definidos por el Departamento Administrativo de la Función Pública – DAFP a la Entidad.

La gestión de riesgos ofrece a la Administración Municipal un método sistemático para analizar los riesgos derivados de los procesos y del uso de las tecnologías de la información y comunicaciones, con el objetivo de descubrir y planificar el tratamiento oportuno, mantener los riesgos bajo control.

4.5.6. Programas de Sensibilización y/o Formación de Empleados

El documento plan de sensibilización presenta la planeación para realizar el programa de sensibilización y/o formación sobre Seguridad de Información dentro de la Administración Municipal, el cual tiene como objetivos principales, lograr que el personal entienda y se comprometa con todos los aspectos relacionados con el Sistema de Gestión de Seguridad de la Información, a partir de la creación de una cultura relacionada con la integridad, confidencialidad y disponibilidad de la información, en donde todos los miembros de la entidad comprendan la importancia de dar un tratamiento adecuado a la información y finalmente concientizar a las personas de los riesgos que se pueden presentar tanto para ellas como para la Entidad.

Gestión de los Recursos del SGSI-MSPI

Es compromiso de la directora de Indersantander garantizar los recursos tanto presupuestales como de personal para la implementación exitosa del SGSI - MSPI.

5.HACER

5.1. Operación

En esta fase se lleva a cabo el establecimiento de los controles de seguridad escogidos en la fase anterior junto con los seguimientos, actualizaciones y procesos de mejora. Dentro de esta fase se destaca el cumplimiento del plan de sensibilización, que conlleva a la concientización y/o formación del personal de la Administración Municipal.

5.2. Métricas de Eficacia de los Controles y del Sistema.

Toda vez que el SGSI-MSPI es un sistema de mejora continua, hay necesidad de definir parámetros precisos para evaluar los controles ejecutados y en sí, la evolución del sistema en términos de justificar cada una de las acciones tomadas o en su defecto redirigir dichas acciones hacia la consecución de procesos más eficientes y efectivos para esto el Indersantader deberá formular indicadores de gestión del MSPI.

5.3. Gestión de Incidentes de Seguridad

El Instituto Departamental De Recreación Y Deportes de Santander formulara el plan de gestión de incidentes para detectar y gestionar un incidente, definido como toda aquella actividad ejecutada como resultado de eventos adversos e inesperados que ocurran como resultado de controles fallidos o inexistentes, teniendo en cuenta las directrices adelantadas por MINTIC, la Policía Nacional y los entes competentes en esta área.

6. VERIFICAR

6.1. Evaluación de Desempeño

Indersantanader dispone de mecanismos que le permitan evaluar la eficacia y éxito de los controles implementados:

- Implementa procedimientos y demás controles de supervisión y control para determinar cualquier violación, procesamiento incorrecto de datos y

determinar si las actividades de seguridad se desarrollan de acuerdo con lo previsto.

- Revisa periódicamente la eficacia del SGSI-MSPI mediante la evaluación y análisis de los indicadores.
- Revisa periódicamente el estado de los activos de información, actualizando periódicamente la matriz correspondiente y la matriz de riesgos
- Realiza Auditorías internas planificadas.
- Actualiza los planes de seguridad para tener en cuenta otras actividades de supervisión y revisión en el caso que sea necesario.

7.ACTUAR

7.1. Mejora Continua

En esta fase se llevarán a cabo las labores de mantenimiento y mejora del sistema de gestión de seguridad de información, seguimiento a riesgos, análisis de vulnerabilidades, así como las labores de mejora y de corrección:

- Implementa y documenta en el SGSI-MSPI las mejoras identificadas.
- Toma medidas correctivas y preventivas y aplica las mejores prácticas sobre incidentes de seguridad, provenientes de experiencias de seguridad propias y de terceros documentadas.
- Comunica las actividades y mejoras a todos los grupos de interés.
- Busca que las mejoras cumplan los objetivos previstos y que estén enfocadas a las necesidades y requerimientos de la Entidad.

8.Plan de Acción 2024

EJE	ÁREA	DESCRIPCIÓN	ENTREGABLE	1 SEMESTRE						2 SEMESTRE					
				E	F	M	A	M	J	J	A	S	O	N	D
Transformación digital	Seguridad para los Servicios ciudadanos digitales (sistemas digitales)	Documentar el manual de seguridad de la información para la protección de los datos personales en sistemas de información que realicen tratamiento de datos personales.	Manual Actualizado de protección de datos personales para sistemas de información con información de carácter personal.												
Riesgos	Tratamiento de Riesgos de Seguridad Digital y Privacidad de la Información	Actualización de los lineamientos de Riesgos de Seguridad de la Información en la Política de administración del Riesgos institucional.	Política Actualizada												
		Incluir dentro del plan de capacitación-PIC 2024 los riesgos de Seguridad digital y privacidad de la información.	Registro del PIC 2024												
		Establecer reuniones con los líderes de los procesos previamente identificando los Riesgos de Seguridad de la Información por proceso.	Riesgos de seguridad digital por proceso												

		Socializar los Riesgos de Seguridad de la Información ante el Comité Institucional de Gestión y Desempeño	Registro de asistencia del comité											
		Realizar monitoreo al cumplimiento de las acciones de control los Riesgos de Seguridad de la Información de la Entidad.	Informe de monitoreo											
		Realizar informe de Seguimiento al cumplimiento de las acciones de control los Riesgos de Seguridad de la Información de la Entidad.	Informe semestral de seguimiento											
Sensibilización	Sensibilización Funcionario y contratistas	Realizar sesiones de sensibilización sobre seguridad de la información y controles del sistema de gestión de seguridad de la información institucional para el equipo de contratistas de la Entidad.	Registro de sensibilizaciones											
	Reinducción e inducción de funcionarios (apoyo a GGH)	Apoyar las actividades de inducción y reinducción de los funcionarios y contratistas de la entidad con charlas en materia de seguridad de la información, protección de datos personales y controles del sistema de gestión.	Registros de asistencia											
Ciberseguridad-OTIC	Centro de respuesta a	Servir como punto de Contacto técnico con el Ministerio de las tecnologías de	Informe de participación en actividades de											

	incidentes de seguridad	información y las comunicaciones en materia de seguridad Digital.	seguridad digital adelantadas por MINTIC											
	Seguridad en la Nube	Acompañar el diseño de lineamientos y controles de seguridad que mitiguen los riesgos que puedan impactar la infraestructura de servicios de nube.	Lineamientos de seguridad para el uso de plataformas de nube											
Gestión de la documentación -MIPG	Diseño de los procedimientos de seguridad de la información	Elaborar los procedimientos del sistema de gestión de seguridad de la información requeridos por la Norma ISO 27001 y el modelo de seguridad y privacidad de la Información recomendado por el Ministerio de las Tecnologías de la Información y las Comunicaciones.	Procedimientos documentados											

BIBLIOGRAFÍA

- Decreto 103 de 2015 el cual reglamenta la ley 1712 de 2014 Ley de Transparencia.

- Ley 1581 de 2012, reglamentada parcialmente por el Decreto Nacional 1377 de 2013 y por el Decreto 1081 de 2015, Protección de datos personales

- Decreto único reglamentario 1078 de 2015 – MinTic – Modelo de Seguridad y Privacidad de Información.

- ISO/IEC 27000:2013. Estándar del Sistema de Gestión de Seguridad de Información.

- MINTIC: https://www.mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Transparencia/135830:Plan-de-seguridad-y-privacidad-de-la-informacion

Aprobó: Comité Institucional de Gestión y Desempeño