POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2021

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.

Tel: 6567702 • 6567677
Fax: 6567708 • 6567709

www.IDER.gov.co

TABLA DE CONTENIDO

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.
Tel: 6567702 • 6567677
Fax: 6567708 • 6567709
www.IDER.gov.co

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.

Tel: 6567702 • 6567677
Fax: 6567708 • 6567709

www.IDER.gov.co

INTRODUCCIÓN

La información en el IDER es identificada como un activo indispensable para el cumplimiento de los procesos, por esta razón se hace necesario establecer un marco en el cual se pueda garantizar que la información está siendo protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Este documento describe las políticas y procedimientos de seguridad y privacidad de la información definidos por el IDER, el cual se constituyen como parte fundamental del Modelo de Seguridad y Privacidad como elemento habilitador de la Política de Gobierno Digital.

2. OBJETIVO

Establecer políticas y procedimientos de seguridad y privacidad de la información, que deben cumplir los funcionarios y contratistas del IDER, para proteger adecuadamente los activos de información que se manejan al interior de la entidad.

3. ALCANCE

Este documento adopta el alcance de la política de seguridad y privacidad de la información de la entidad.

4. TÉRMINOS Y DEFINICIONES

Para propósitos de este documento se aplican los términos y definiciones presentados a continuación.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Ciberseguridad**: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3995).

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.
Tel: 6567702 • 6567677
Fax: 6567708 • 6567709
www.IDER.gov.co

• **Ciberespacio**: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
• **Control** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

• **Riesgo:** 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).

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.
Tel: 6567702 • 6567677
Fax: 6567708 • 6567709
www.IDER.gov.co

5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

El Instituto Distrital de Deporte y Recreación - IDER, entendiendo la importancia de sus activos de información para el cumplimiento de su misión institucional, se ha comprometido con la implementación del modelo de Seguridad y privacidad de la Información (MSPI) buscando proteger la confidencialidad, integridad y disponibilidad de los activos de información y además establecer un marco de confianza en el ejercicio de su misión con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes aplicables.

El Instituto Distrital de Deporte y Recreación - IDER en su propósito de dar cumplimiento con la política de seguridad y privacidad de la información, establece los siguientes objetivos:

5.1 OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, y en los grupos de interés que tienes algún vínculo con el IDER.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Minimizar el riesgo de todos los procesos de la entidad.
- Mejorar continuamente el modelo de seguridad y privacidad de la información.
- Implementar los controles tecnológicos necesarios para la protección de los activos de la entidad y para la reducción de los riesgos.

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.
Tel: 6567702 • 6567677
Fax: 6567708 • 6567709
www.IDER.gov.co

6. COMPROMISO DE LA ALTA DIRECCIÓN

La Dirección general del Instituto Distrital de Deporte y Recreación – IDER, se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Modelo de Seguridad y Privacidad de la Información (MSPI); así mismo, se compromete a revisar el avance de la implementación del MSPI de manera periódica y también garantizará los recursos suficientes (tecnológicos y talento humano calificado) para implementar y mantener el modelo, así mismo, incluirá dentro de las decisiones estratégicas, la seguridad de la información.

7. APLICABILIDAD

La presente política, sus objetivos, además de los manuales, procedimientos o documentos derivados o complementarios aplican a toda la entidad, servidores públicos, contratistas y terceros del Instituto Distrital de Deporte y Recreación – IDER.

El incumplimiento a la Política de Seguridad y Privacidad de la Información o de sus lineamientos derivados, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad.

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.
Tel: 6567702 • 6567677
Fax: 6567708 • 6567709
www.IDER.gov.co

8. ROLES Y RESPONSABILIDADES

El Instituto Distrital de Deporte y Recreación – IDER, define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados (Manuales, Procedimientos, Planes, Formatos etc.…):

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (DEBERES RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN)
Alta Dirección	• Proporcionar los recursos necesarios para la implementación y mantenimiento del modelo de seguridad y privacidad de la información (Recursos económicos, formación y recursos tecnológicos).
Comité de Gestión y Desempeño	• Aprobar los recursos correspondientes para la implementación y el mantenimiento del modelo de seguridad y privacidad de la información.
Grupo TIC / Oficial de Seguridad Digital	• Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información. • Analizar, definir, documentar y gestionar el plan estratégico de seguridad de la información y proponer las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidas y aprobados por la entidad. • Apoyar en la generación de los lineamientos (Manuales, procedimientos y formatos) que permitan el establecimiento y mejoramiento continuo del Modelo de Seguridad y Privacidad de la Información en la Entidad.
Talento Humano	• Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos.
Control Interno	• Incluir la seguridad de la información, dentro de los planes de auditoría institucionales. • Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información.
Prensa / Comunicación Interna	• Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la entidad.

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.
Tel: 6567702 • 6567677
Fax: 6567708 • 6567709
www.IDER.gov.co

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (DEBERES RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN)
Oficina de Contratación	• Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad. • Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos.
Líderes de Proceso	• Implementar las políticas y procedimientos de seguridad de la información que se definan como parte del MSPI (Por ejemplo: gestión de activos, gestión de riesgos, entre otros).
Todos los funcionarios y contratistas	• Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos. • Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados.

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.

Tel: 6567702 • 6567677
Fax: 6567708 • 6567709

www.IDER.gov.co

9. SANCIONES

Cualquier violación a las políticas de seguridad de la información del Instituto Distrital de Deporte y Recreación – IDER, debe ser sancionada de acuerdo con el Reglamento Interno de Trabajo, a las normas, leyes y estatutos de la ley colombiana, así como la normativa atinente y supletoria, y apoyados en las leyes regulatorias de delitos informáticos de Colombia.

10. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL MSPI

El Instituto Distrital de Deporte y Recreación – IDER, indica que realizará revisiones periódicas al MSPI. Dichas revisiones estarán enfocadas en los siguientes aspectos:

- Revisión de indicadores definidos para el Modelo de Seguridad y Privacidad de la Información.
- Revisión de avance en la implementación del Modelo de Seguridad y Privacidad de la Información del IDER.
- Revisión de avance de la Política de Seguridad Digital de acuerdo con lo solicitado por FURAG o la herramienta definida para tal fin.

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.

Tel: 6567702 • 6567677
Fax: 6567708 • 6567709

www.IDER.gov.co

11. MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

11.1. POLÍTICA DE DISPOSITIVOS MÓVILES

Llevar un registro y control de todos los dispositivos móviles (portátiles, tabletas y teléfonos móviles) que posee el IDER. (Entrega y recibido de los dispositivos) y hacer firmar por parte del servidores públicos y contratistas el compromiso de cumplimiento de controles.

11.1.1 Acceso a la red "DIRECCION_XX"

- El IDER permite el uso de dispositivos móviles de funcionarios y contratistas los cuales requieren de los servicios de red de la entidad para el desarrollo de sus obligaciones contractuales.
- La oficina de tecnología es la responsable de autorizar el acceso a la red "**DIRECCION_XX**.

11.1.2 Acceso a la red "IDER_V" (Para Invitados)

- El IDER permite el uso de dispositivos móviles de ciudadanos y visitantes de las instalaciones de la entidad.

11.2. POLÍTICA DEL USO ACEPTABLE DE LOS ACTIVOS

Los equipos de cómputo de la entidad serán responsabilidad del funcionario o contratista, que, para el desarrollo de sus funciones, se le haya asignado mediante procedimiento establecido para esto.

El usuario deberá tomar las medidas de seguridad pertinentes que permitan garantizar la integridad y confidencialidad del activo de información.
En caso de presentarse una falla o problema de hardware o software en una estación de trabajo o equipo portátil propiedad del IDER, el usuario responsable del mismo deberá informarlo a la oficina de sistemas, para una asistencia especializada y, por ningún motivo, deberá intentar resolver el problema.

Los artículos de decoración no son permitidos sobre las estaciones de trabajo o equipo portátil de la entidad. Se debe mantener el equipo de cómputo libre de fotos, calcomanías y cualquier otro elemento que pueda deteriorar o comprometer la integridad del activo. El funcionario o contratista se hace responsable por los daños o pérdidas de los equipos tecnológicos asignados, los cuales debe devolver una vez este desvinculado de la entidad.

11.3. POLÍTICA DE CONTROL DE ACCESO

El control de acceso a todos los Sistemas de Información de la entidad y en general cualquier servicio de Tecnologías de Información, debe realizarse por medio de credenciales de acceso (usuario y contraseña), las cuales son de uso exclusivo e intransferible.
Crear y/o deshabilitar usuarios de acceso a los sistemas de información se hará de acuerdo con el procedimiento que indica la vinculación o desvinculación del funcionario o contratista en la entidad.

Sistemas de información:

- SIGOB
- SAFE
- Directorio activo

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.
Tel: 6567702 • 6567677
Fax: 6567708 • 6567709
www.IDER.gov.co

- Correo institucional
- Sitio WEB
- Redes sociales

La asignación de la contraseña para acceso a sistemas se debe realizar de forma individual, por lo que el uso de contraseñas compartidas está prohibido. Al revelar o compartir la contraseña el usuario autorizado se expone a responsabilizarse de acciones que otras personas hagan con su contraseña.

Los usuarios no deben almacenar las contraseñas en ningún lugar, programa o sistema que proporcione facilidad de acceso a personas no autorizadas sin su conocimiento.

11.4. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

Esta política se aplica a la protección de cualquier tipo de información, cualquiera de sus formas y que pueden estar contenidas en escritorios, estaciones de trabajo, computadores portátiles, medios ópticos, medios magnéticos, documentos en papel y en general cualquier tipo de información que se utiliza para los procesos estratégicos, misionales y de apoyo de la entidad.

Todas las estaciones de trabajo deben contar con bloqueo de sesión automática después de 5 minutos de inactividad, el cual, debe mostrar la pantalla de inicio de sesión solicitando el ingreso del usuario y contraseña al ser reanudado.

La información, cuando se imprime se debe retirar inmediatamente de las impresoras.

El funcionario o contratista al ausentarse de su lugar de trabajo debe bloquear su estación de trabajo para proteger el acceso de personal no autorizado.

Al finalizar la jornada de trabajo, el usuario debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno, así mismo debe cerrar la sesión o salir de todas las aplicaciones correctamente y dejar los equipos apagados (no sólo el monitor). Se exceptúa los funcionarios de la oficina de sistemas, quienes en alguna ocasión requieren dejar corriendo procesos en horas de la nocturnas.

Sobre los escritorios u oficinas abiertas y durante la ausencia de los funcionarios o contratistas no deben permanecer a la vista documentos en papel, dispositivos de almacenamiento como cd, memorias USB, etc., con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante el horario laboral y fuera del mismo.

11.5. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Todas las personas que ingresen a las instalaciones de la entidad deben portar carnet de identificación, ya sea como funcionarios, contratistas o visitantes.

- Centro de datos
- Archivos
- Áreas restringidas

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.
Tel: 6567702 • 6567677
Fax: 6567708 • 6567709
www.IDER.gov.co

11.6. POLÍTICA RESTRICCIONES SOBRE INSTALACIONES Y USO DEL SOFTWARE

El personal adscrito a la oficina de sistemas es el único autorizado para instalar aplicaciones y realizar mantenimientos preventivos y correctivos en los equipos de cómputo de la entidad.

Para todos los equipos de cómputo propiedad del IDER, se instalará únicamente el software que cuente con licencia autorizada para uso en la entidad. El software que no cumpla con estos lineamientos se debe desinstalar de manera inmediata para garantizar el cumplimiento de la Ley.

Para todos los equipos de cómputo propiedad de IDER, se instalará únicamente el software antivirus que la oficina de sistemas establezca.

Los usuarios que hacen uso de los servicios de tecnología de información y comunicación deben realizar tareas de escaneo de archivos y directorios, además, no deben cambiar o eliminar la configuración del software de antivirus en los equipos de cómputo propiedad de la entidad.

Los usuarios no deben descargar archivos adjuntos que provengan de fuentes desconocidas, para evitar contaminación por código malicioso en sus estaciones de trabajo o equipos portátiles.

La suite de ofimática permitida por la entidad para equipos con sistema operativo Windows y Mac, son las versiones de Microsoft Office licenciadas por la entidad. Se permite el uso de la versión libre de WPS Office 2016 Free, en los equipos de cómputo propiedad del IDER.

La entidad se reserva el derecho de monitorear los equipos de cómputo, conectados a la red de datos del IDER, de los cuales se sospeche que están comprometiendo la confidencialidad, integridad y disponibilidad de la información.

Los usuarios no pueden portar información de la entidad clasificada como privada sin la previa autorización del propietario del activo de información independiente del medio que utilice.

Está prohibido almacenar información personal en los equipos de cómputo propiedad de IDER.

11.7. POLÍTICA DE COPIAS DE RESPALDO

Toda la información contenida en los equipos de cómputo, estarán adheridos al drive de Google, permitiendo automatizar la protección de la información en la nube de la entidad y a su vez serán sincronizados automáticamente.

Sistemas de información:
- SIGOB
- SAFE
- Directorio activo
- Correo institucional
- Sitios WEB Institucionales

11.8. POLÍTICA DE GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS

Las violaciones a las políticas y controles de seguridad y privacidad de la información serán reportadas, registradas y monitoreadas por el oficial de seguridad y privacidad de la información,

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.
Tel: 6567702 • 6567677
Fax: 6567708 • 6567709
www.IDER.gov.co

mediante procedimiento, garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad y privacidad.

Cualquier brecha en la seguridad o sospecha en la mala utilización en el Internet, la red o los recursos informáticos de cualquier nivel debe ser comunicada por el funcionario o contratista que la detecta en forma inmediata y confidencial al oficial de seguridad y privacidad de la información.

11.9. POLÍTICA PARA LAS RELACIONES CON CONTRATISTAS

- Los contratistas protegerán la información a la que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentre contenida esa información.
- Para obtener el acceso a los activos de información será necesario disponer de un acceso autorizado, por medio del procedimiento que este establecido por la entidad.
- Ningún contratista en proyectos o trabajos puntuales deberá poseer, para usos no propios de su responsabilidad, material alguno o información propia o confiada al IDER tanto ahora como en el futuro.
- En el caso de que, por motivos directamente relacionados con el trabajo, el empleado del contratista prestador del servicio entre en posesión de información confidencial contenida en cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.
- Esta política continuará vigente tras la finalización de las actividades que el contratista desarrolle para el Instituto.

11.10.POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

Para conocer esta política ingresa aquí.

11.11. POLÍTICA DE "CERO PAPEL"

El concepto de "cero papel" se relaciona con la reducción sistemática del uso del papel mediante la sustitución de los flujos documentales en papel por soportes y medios electrónicos. La estrategia Cero Papel no concibe la eliminación radical de los documentos en papel. Las entidades deberán identificar y aplicar buenas prácticas para reducir el consumo de papel, de acuerdo con la Guía que ya está disponible en la política de gobierno digital y los lineamientos de la directiva presidencial 4 de 2012.

11.12. POLÍTICA PARA EL MANEJO DE LA INFORMACION

11.12.1. Acuerdos de confidencialidad

Todos los funcionarios y contratista deben conocer, entender, firmar y aceptar un acuerdo de confidencialidad, donde se comprometan a no divulgar, usar o explotar la información a la cual tenga acceso. De igual manera se compromete a proteger y hacer buen uso de esta, respetando los niveles de clasificación en cuanto a criticidad y protección, por consecuente cualquier violación de lo establecido será considerado un incidente de seguridad y tendrá su sanción dependiendo la magnitud de los hechos.

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.
Tel: 6567702 • 6567677
Fax: 6567708 • 6567709
www.IDER.gov.co

11.12.2. Propietario de la información

La información (bases de datos, documentos, videos, fotos, papelería de créditos, entre otros) administrada, manejada o creada por el IDER, es propiedad de la entidad, quien tiene todos los derechos de esta información.

11.12.3. Derechos de autor

Está prohibido hacer copias de la información de la entidad en cualquier formato, copias no autorizadas de software ya sea adquirido o desarrollado por la entidad. De igual forma, el IDER no realizará copias de seguridad de software que no le esté permitido.

11.12.4. Correo institucional

Debe ser usado para el desempeño de las funciones asignadas dentro del IDER. Los usuarios no deben propagar cadenas de mensajes de cualquier tipo y la comunicación de tipo comercial, político, religioso y en general cualquier contenido ofensivo para los funcionarios de la entidad. Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por el IDER.

Es deber de los funcionarios y contratistas verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

11.13. POLÍTICA DE INSTALACION DE CABLEADO

Planeación, diseño, construcción, instalación, administración y mantenimiento del cableado estructurado de telecomunicaciones de la entidad es responsabilidad de la oficina de sistemas, y debe cumplir con las normas técnicas o estándares adoptados por el mismo, con el fin de garantizar la integridad, conservar la estética y la seguridad de las redes.

11.14. POLÍTICA DE GESTION DE MEDIOS REMOVIBLES

Los medios removibles NO son una alternativa de respaldo de información permanente, siendo responsabilidad de los usuarios mantener la información en los servidores, servicios en la nube de Google Drive o equipos destinados para ello.

Los medios removibles deben ser escaneados cada vez que sea conectado a un equipo del IDER, especialmente en lo concerniente a posible código malicioso.

Debe formatearse el medio removible cuando la información pierda vigencia.

El funcionario o contratista debe dar buen uso a los medios removibles asignados, informando oportunamente cualquier deterioro.

No se debe almacenar información confidencial en los teléfonos móviles.

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.
Tel: 6567702 • 6567677
Fax: 6567708 • 6567709
www.IDER.gov.co

Una vez asignado el medio removible al usuario, es de su exclusiva responsabilidad tomar las medidas adecuadas para el almacenamiento y custodia necesarios de la información, para protegerla de accesos no autorizados, daño o pérdida.

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.

Tel: 6567702 • 6567677
Fax: 6567708 • 6567709

www.IDER.gov.co

12. SENSIBILIZACIÓN Y COMUNICACIÓN

El plan de sensibilización está diseñado para dar a conocer los riesgos a los que las aplicaciones, la infraestructura, los servicios, los usuarios, las redes y la información en general están expuestos, y generar dentro de todos los funcionarios y contratistas buenas prácticas respecto a la seguridad de la información, estás buenas prácticas actúan de manera preventiva ayudando a la entidad a salvaguardar sus activos de información.

Con el uso de la tecnología, surgen a su vez amenazas y vulnerabilidades asociadas, que pueden llegar a afectar la disponibilidad, privacidad e integridad de la información que se encuentra disponible en las diferentes plataformas, afectando de esta manera el desempeño normal de la entidad.

Muchas instituciones no prestan la suficiente atención a su recurso humano, que puede llegar a ser el eslabón más débil en la cadena de la seguridad de la información, por lo que es necesario sensibilizarlos o capacitarlos sobre la importancia de la preservación de la disponibilidad, integridad y confidencialidad de la información.

Para llevar a cabo la ejecución del plan de sensibilización de seguridad de la Información se ha desarrollado un cronograma con las actividades para ser ejecutadas durante la vigencia del 2021, las actividades que se tienen programadas son las siguientes:

No	ACTIVIDAD	TEMA	CANAL DE COMUNICACIÓN	HERRAMIENTAS	FRECUENCIA
1	Charla de sensibilización	Manual de políticas de seguridad y privacidad de la información.	Comunicaciones al interior de la entidad.	Presentaciones y piezas graficas	2 al año
2	Realizar campañas de sensibilización de riesgos de ciberseguridad y privacidad de la información (Noticias, Tips y Alertas de Seguridad).	**Amenazas Informáticas**: Phishing, Malware, Ramsonware entre otros. **Seguridad en estaciones de trabajo:** Escritorios limpios, pantallas limpias, contraseñas seguras, etc. **Respaldo de la información:** Copias de seguridad (Backup). Otras recomendaciones de seguridad.	Comunicaciones al interior de la entidad.	*Piezas gráficas, Campañas de correo electrónicos, Redes sociales.	1 al mes
3	Realizar ejercicios de simulación de incidentes de seguridad digital al interior de la entidad.	Generar cultura y enseñar a los funcionarios del IDER, medidas de protección ante posibles ataques cibernéticos.	Todos los funcionarios		2 al año

Cronograma de Actividades

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.
Tel: 6567702 • 6567677
Fax: 6567708 • 6567709
www.IDER.gov.co

13. APROBACIÓN Y REVISIONES A LA POLÍTICA

Esta política será efectiva desde su aprobación por el comité de gestión y desempeño. La revisión de esta política se hará en las siguientes condiciones:

1. De forma anual, donde se deberá revisar la efectividad de la política y sus objetivos.
2. Si se dan cambios estructurales en la entidad (restructuración de áreas o procesos).
3. Incidentes de seguridad de la información que requieran que la política necesite cambios.

14. VIGENCIA Y CONTROL DE CAMBIOS

FECHA	AUTOR	VERSION	CAMBIOS
01 de junio 2021	Oficina de TIC	1.0	Versión inicial.

Cartagena de Indias
Colombia - Pie de la Popa
Cra.30 No.18A-253.
Tel: 6567702 • 6567677
Fax: 6567708 • 6567709
www.IDER.gov.co