TABLA DE CONTENIDO

1. INTRODUCCIÓN

En lineamiento con MIPG, el Instituto Municipal Para el Desarrollo Social y Económico de Palmira -IMDESEPAL en el uso masivo de las Tecnológicas de la información y las comunicaciones (TIC), se identifica como base para las actividades socioeconómicas e incrementando la participación digital de los ciudadanos, generando diferentes alternativas para atentar contra la seguridad de la entidad y el estado; Siendo necesario fortalecer la capacidad del instituto para identificar, gestionar el riesgo y atiende las situaciones para brindar protección en el ciberespacio.

Por medio de la presente política el Instituto Municipal Para el Desarrollo Social y Económico de Palmira -IMDESEPAL dispondrá estrategias que permiten resolver problemas y generar diagnósticos más rápidamente en los escenarios de riesgos de la entidad.

2. OBJETIVO

Identificar los riesgos en el entorno digital del Instituto Municipal para el Desarrollo Social y Económico de Palmira

Objetivo especifico

Formular un plan de acción para la protección, prevención y reacción ante delitos y ataques cibernéticos.

Fomentar la cultura de consciencia del manejo del riesgo cibernético de la entidad

3. NORMATIVIDAD

De acuerdo con MIPG, se reglamenta la siguiente normatividad:

- Acuerdo 08 de 2019
- Ley 1928 de 2018
- Acuerdo 02 de 2018
- Conpes 3854 de 2016
- Decreto 1078 de 2015
- Ley 1712 de 2014 - Transparencia y Acceso a la Información Pública
- Ley estatutaria 1581 de 2012
- Decreto 103 de 2015
- Ley 1273 de 2009

4. ALCANCE

El alcance incluye la prevención de riesgos digitales, alineado a MIPG en la tercera dimensión de Gestión con Valores para Resultados.

5. IDENTIFICACIÓN DE RIESGOS DIGITALES

EXTERNOS

- Ataque digital
- Daños al hardware y software de la entidad

INTERNOS

- Falta de conocimiento en los riesgos digitales
- Ingreso de dispositivos con virus a los computadores y correos de la entidad como (USB, celulares)
- Perdida de la información por daño en equipos.

6. PREVENCIÓN DE RIESGOS DIGITALES

- Concientizar a los empleados y/o contratistas de las consecuencias
- Adoptar buenas prácticas en el comportamiento del cibernauta

En recomendación de MINTIC, a la ciudadanía en general, empleados y/o contratistas de la entidad se dictamina lo siguiente:

- No descargar archivos sospechosos.
- Actualizar el software del sistema periódicamente.
- Usar antivirus y aplicaciones anti-malware.
- Crear mejores contraseñas y cambiarlas cada seis meses.
- Acostumbrar a cerrar las sesiones al terminar.
- Evitar operaciones privadas en redes abiertas y publicas.
- Desconectarse de internet cuando no se necesite.
- Realizar copias de seguridad.
- Navegar por páginas web seguras y de confianza.
- Comprobar la seguridad de la red WIFI.
- No hacer clic en enlaces raros.
- No dar datos personales a desconocidos.
- En las empresas se debe hacer una política de seguridad corporativa.

La denuncia de los delitos cibernéticos si un ciudadano es víctima de delitos electrónicos financieros podrá denunciar en el CAI Virtual, en la página web www.ccp.gov.co

Conocer los riesgos y saber cómo actuar frente a ellos es clave en la vida digital. Por ello, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), a través de la iniciativa que promueve el uso responsable de las TIC y el

grupo de Seguridad de la Información de Gobierno Digital, se une a la conmemoración del Día Internacional del Internet Seguro con un decálogo de recomendaciones para prevenir los riesgos en los entornos digitales.

1. No responda ni de clic a enlaces que reciba de remitentes desconocidos; primero asegúrese de que se trata de una fuente confiable.

2. Cambie sus contraseñas de forma regular, evite usar la misma en todas las cuentas que tenga, así como datos evidentes como su nombre, teléfono o fecha de nacimiento.

3. Use contraseñas que no sean de fácil acceso para los criminales y sean sencillas de aprender, escogiendo frases hechas con al menos cuatro palabras que no tengan relación alguna.

4. No deje sus redes sociales abiertas en equipos de uso público.

5. Tenga en cuenta las clasificaciones de privacidad que las redes sociales ofrecen a la hora de publicar contenido.

6. No comparta todo lo que recibe, analice y verifique la veracidad de la información antes de difundirla entre sus allegados.

7. Evite aceptar personas que no conoce en sus redes sociales, así tengan muchos amigos en común.

8. No publique todo lo que hace, ni todos los lugares a los que va. Tenga en cuenta que esa es información que los delincuentes pueden usar.

9. Evite intercambiar fotografías, videos o mensajes íntimos a través de Internet. Recuerde que puede convertirse en contenido para otros riesgos como el ciberacoso o el grooming.

10. Evite tener encuentros con personas que haya conocido en los entornos digitales; tenga en cuenta que siempre existe la posibilidad de que sea un perfil falso.

7. POLÍTICAS DE SEGURIDAD DIGITAL

7.1. Política de organización interna

Establecer un marco de referencia de gestión para iniciar y controlar la implementación de la seguridad digital al interior del Instituto Municipal Para el Desarrollo Social de Palmira- IMDESEPAL por medio de la definición de roles y responsabilidades en seguridad digital, la separación de deberes, el contacto con las autoridades y grupos de interés y la incorporación de la seguridaddigital en la gestión de los proyectos, todo ello alineado con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de TIC, buscando preservar la confidencialidad, integridad y disponibilidad de la información.

Alcance

La Política de Organización Interna aplica a todos los colaboradores y terceros de IMDESEPAL

7.2. Política para dispositivos móviles

Establecer los lineamientos para el buen uso y administración de los equipos de computación y comunicación móvil asignados o autorizados a los colaboradores del IMDESEPAL, para el desarrollo de sus funciones, y así asegurar la confidencialidad, la integridad y la disponibilidad de la información del IMDESEPAL contenida en estos.

Alcance

La política para uso de dispositivos móviles será aplicada todos los colaboradores y terceros que utilicen dispositivos móviles para acceder a los servicios ofrecidos por el IMDESEPAL (red, Internet, correo electrónico, sistemas deinformación etc.)

7.3. Política de seguridad de los recursos humanos

Asegurar que los colaboradores y terceros comprendan y tomen conciencia sobre sus responsabilidades de seguridad de la información y las cumplan, además asegurar que son idóneos en los roles asignados y que se protegen los intereses del IMDESEPAL como parte del proceso de cambio de vinculación o terminación de esta.

Alcance

La política de seguridad de los recursos humanos debe ser cumplida por todos los colaboradores y terceros de todos los procesos de IMDESEPAL; cubre los objetivos de control (Norma ISO 27001): antes de asumir, durante la ejecución y la terminación o cambio de la vinculación a IMDESEPAL.

7.4. Política de uso adecuado de los recursos

Dar un buen uso a los recursos: correo electrónico, internet, redes sociales, recursos tecnológicos (Equipo de cómputo), uso de software legal y derechos de autor, acceso inalámbrico que provee IMDESEPAL a todos los colaboradores y terceros para el cumplimiento de sus funciones u obligaciones, y para proteger la información del IMDESEPAL. No es una red de acceso público.

Alcance

Aplica para todos los colaboradores y terceros vinculados con IMDESEPAL que tienen acceso a los servicios de correo electrónico, acceso a internet, redes sociales, recursos tecnológicos (Equipos de cómputo), uso de software legal y derechos de autor, acceso inalámbrico para el desarrollo de sus funciones.

7.5. Política de gestión de activos de información

Identificar los activos de información de IMDESEPAL para definir las responsabilidades de protección apropiadas y clasificarlas para asegurar que la información del IMDESEPAL recibe un nivel apropiado de protección, de acuerdo con su importancia, y se efectúe un manejo adecuado de los medios para evitar la divulgación, modificación, el retiro o la destrucción no autorizada de la información de IMDESEPAL almacenada en ellos.

Alcance

Aplica para los activos de información de todos los procesos del IMDESEPAL siendo contemplada en el Plan Estratégico de Tecnología de la Información

7.6. Política de control de acceso

Definir las directrices generales para un acceso controlado a servicios de tecnología(Red, servicios asociados, sistemas de información) e información de IMDESEPAL.

Alcance

Esta política aplica para todos los colaboradores y terceros que cuenten con accesos a los servicios de tecnología (Red, servicios asociados, sistemas de información) e información de IMDESEPAL.

7.7. Política de seguridad física y del entorno

Minimizar los riesgos de daños e interferencias a la información y a las operaciones de IMDESEPAL, evitando accesos físicos no autorizados a las instalaciones de procesamiento de información, que atenten contra la confidencialidad, integridad odisponibilidad de la información del IMDESEPAL.

Alcance

Esta política aplica para el control de acceso físico a las áreas seguras dentro de las cuales se encuentran el centro de datos, centros de cableado, áreas de archivo,áreas de recepción, tesorería, despachos y entrega de correspondencia, las cualesdeben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información de IMDESEPAL.

7.8. Política de escritorio y pantalla limpios

Mantener el escritorio y la pantalla despejada, con el fin de reducir el riesgo de acceso no autorizado, pérdida y daño de la información del IMDESEPAL.

Alcance

Esta política aplica para todos los colaboradores y terceros de IMDESEPAL contemplada en la política del sistema de gestión y seguridad de la información

7.9. Política de gestión de seguridad de las redes

Fortalecer la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte de IMDESEPAL

Alcance

Esta política aplica para todas las redes, los servicios de red y los controles utilizados para proteger la información en la transferencia de información de IMDESEPAL.

7.10. Política de intercambio de información

Proteger la transferencia de información del IMDESEPAL mediante el uso de todo tipo de instalaciones de comunicación, como correo electrónico, VPN, SFTP, etc.

Alcance

Esta política de intercambio de información aplica para la información que sea enviada por los colaboradores a través de correo electrónico y los demás canales que se autoricen VPN, SFTP, etc.

7.11. Política de adquisición, desarrollo y mantenimiento de sistemas

Fortalecer la seguridad digital y que sea una parte integral de los sistemas de información de IMDESEPAL durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.

Alcance

Esta política aplica para todos los sistemas de información de IMDESEPAL, incluyendo los sistemas de información que prestan servicios sobre redes públicas.

7.12. Política de desarrollo seguro

Propender porque la seguridad digital esté diseñada e implementada dentro del ciclode vida planeación y desarrollo de los sistemas de información.

Alcance

Esta política aplica para todos los desarrollos de sistemas de información en IMDESEPAL.

7.13. Política de seguridad de la información para las relaciones con proveedores

Buscar la protección de los activos información del IMDESEPAL que sean accesibles a losproveedores.

Alcance

Esta política aplica para todos los proveedores que para la ejecución de su trabajo requieran acceder a la información o infraestructura tecnológica de IMDESEPAL.

8. VIGENCIA

Tiene vigencia permanente y será revisada como mínimo una vez al año con el fin de realizar actualizaciones o mejoras que se consideren pertinentes si aplica.

Se debe publicar con una frecuencia anual, y en caso de modificaciones o actualizaciones, se realizará una nueva publicación por los medios dispuestos.

Se aprueba y adopta por medio del comité de gestión y desempeño

9. CONTROL DE CAMBIOS

VERSIÓN	FECHA	ÍTEM MODIFICADO	DESCRIPCIÓN DEL CAMBIO
1	01/12/2021		Creación del documento