POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

DEFINCIÓN

Esta Política de Seguridad de la Información define los lineamientos y medidas a tener en cuenta para gestionar los riesgos de seguridad de la información sobre los activos de información, los procesos y actividades generales de la Asociación.

OBJETO

Salvaguardar la información que se dispone por parte de la organización y con base en el soporte de las tecnologías de la información y comunicación -TIC- para el contacto simultáneo entre todas las partes interesadas, aplicando estos lineamientos para la seguridad de la información de Ascún, a partir de la identificación, evaluación y valoración de los riesgos, para establecer los respectivos controles de los recursos a los que tiene acceso cada responsable y el fomento de la cultura de prevención en términos de seguridad de la información tanto al interior como al exterior.

ALCANCE

La presente política será aplicable a todos los colaboradores de la Asociación que se encuentren vinculados laboralmente, bajo la modalidad presencial y de teletrabajo.

NORMATIVA

Mediante el Decreto 1227 del 18 de julio de 2022, en su artículo 1 que modifica el artículo No. 2.2.1.5.3. Contrato o vinculación de teletrabajo, se especifica en el numeral 1 “Las condiciones necesarias para la ejecución de las funciones asignadas, los medios tecnológicos y de ambiente requeridos, así como la descripción de equipos y programas informáticos, junto con las restricciones y las responsabilidades que pueda acarrear su incumplimiento”.

SANCIONES

El incumplimiento generará las sanciones que establezca la Asociación.

GLOSARIO

- **TICS**: Tecnologías de la Información y las Comunicaciones (TIC), son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes
- **Seguridad de la información:** conjunto de medidas y técnicas para controlar los datos que se manejan al interior de la Asociación y asegurar que éstos no sean publicados fuera del sistema.
- **Teletrabajo:** Una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación -TIC- para el contacto

entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio especifico de trabajo"

- **Aplicaciones:** programa informático diseñado como una herramienta para realizar operaciones o funciones específicas. Generalmente, son diseñadas para facilitar ciertas tareas complejas y hacer más sencilla la experiencia informática de las personas.
- **Virus informático:** tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo. Además, está diseñado para propagarse de un equipo a otro.
- **Códigos maliciosos:** llamado “software malicioso” o “software malintencionado”. Es cualquier software corrupto, dañino, nocivo o no autorizado diseñado para infiltrarse y dañar un sistema informático, incluyendo, con carácter enunciativo, pero no limitativo:
- **Back Up:** Copia de seguridad de uno o más archivos informáticos, que se hace para prevenir posibles pérdidas de información.
- **VPN:** Virtual Private Network o Red Privada Virtual es un método utilizado para conectarnos a Internet de forma privada.

COBERTURA

INFRAESTRUCTURA INFORMÁTICA

- ✓ Actualizar el control de acceso a la infraestructura
- ✓ Combinar dos o más factores de autenticación de acceso directo

TELECOMUNICACIONES

- ✓ Hacer uso de VPN
- ✓ Contar con un firewall

APLICACIONES

- ✓ Cambiar con regularidad claves de acceso
- ✓ Utilizar claves de alta complejidad
- ✓ Establecer procesos seguros de entrega de claves
- ✓ Crear perfiles de acceso a la aplicación
- ✓ Cifrar datos sensibles

DISPOSITIVOS DE USUARIO

- ✓ Actualizar antivirus rutinariamente
- ✓ Activar mecanismos de autenticación
- ✓ Realizar copias de respaldo
- ✓ Cifrar la información sensible

La seguridad de la información se basa en preservar los siguientes aspectos:

- **Confidencialidad:** Garantizar que la información sea accesible solo a aquellas personas autorizadas a tener acceso a la misma.
- **Disponibilidad:** Garantizar que los usuarios autorizados tengan acceso a la información en el momento que la requieran.
- **Auditabilidad:** Registrar todos los eventos de un sistema para su control posterior.
- **No repudio:** Evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la ha enviado o recibido.
- **Integridad:** Salvaguardar la exactitud de la información y métodos de procesamiento de ser alterados por terceros.
- **Autenticidad:** Asegurar la validez de la información y garantizar que el origen de ésta sea válido, evitando suplantación de identidades.
- **Protección a la duplicación:** Asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla con el objeto de simular múltiples peticiones del mismo remitente original.
- **Legalidad**: Cumplimiento de las leyes, normas, reglamentaciones y disposiciones a las que está sujeta la entidad.

ROLES Y RESPONSABILIDADES

La política de seguridad de la información es de aplicación obligatoria para todo el personal de la entidad, el área a la cual pertenezca y cualquiera sea el nivel de las tareas que desempeñe.

ROL	RESPONSABILIDAD
✓ Dirección ejecutiva ✓ Coordinación administrativa y financiera	✓ Aprobar las políticas de seguridad de la información. ✓ Facilitar los recursos requeridos para el sistema de gestión de seguridad de la información.
✓ Todo el personal	✓ Reportar a la coordinación administrativa y financiera, respecto a oportunidades de mejora en materia de Seguridad de la Información, así como los incidentes relevantes y su solución.
✓ Auxiliar de sistemas y telecomunicaciones	✓ Cambiar con regularidad claves de acceso. ✓ Utilizar claves de alta complejidad. ✓ Establecer procesos seguros de entrega de claves. ✓ Crear perfiles de acceso a la aplicación. ✓ Cifrar datos sensibles. ✓ Actualizar antivirus rutinariamente de los sistemas de información de la Asociación (equipos de cómputo, servidor) para evitar el acceso de códigos maliciosos a la información. ✓ Realizar back up de toda la información que se encuentra en los diferentes repositorios de información (correo, drive, VPN).

	✓ Coordinar la asignación de la VPN con las áreas de la Asociación, a fin de apoyar la centralización de la información. ✓ Apoyar a las diferentes áreas en la adopción de la política de seguridad de la información.
✓ Todo el personal	✓ Hacer uso exclusivo de los diferentes repositorios de información y la preservar la conservación de estos. ✓ Actualizar antivirus rutinariamente de los equipos descritos en el acuerdo de compensación para evitar el acceso de códigos maliciosos a la información de la Asociación. ✓ Activar mecanismos de autenticación (correo, VPN).

Esta orientación se complementa con la necesidad de usar repositorios de información que suministra la organización, velar por la configuración de los dispositivos de teletrabajo (sistema operativo, antivirus, control de actualizaciones, etc.), tanto corporativos como los que se encuentran en calidad de préstamo por parte de cada responsable, salvaguardar el manejo de la información que esté a cargo, sin derecho a divulgarla por ningún motivo, y preservar la confidencialidad de esta.

La presente política se revisa y se firma el día 16 de enero de 2023.

Comuníquese, publíquese y cúmplase.

OSCAR DOMÍNGUEZ GONZÁLEZ
Representante Legal

Elaboró: Yesenia Katerin Rojas Moreno, Profesional administrativo y financiero
Aprobó: Carolina Henao Montoya, Coordinadora administrativa y financiera