POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

ASISTENCIA SyS S.A.S.

1. Declaración de compromiso

ASISTENCIA SyS S.A.S., empresa dedicada a la prestación de servicios de asistencia al hogar, asistencia legal y asistencia de transporte, reconoce la información como un activo estratégico para el cumplimiento de sus objetivos corporativos y para la generación de confianza entre clientes, proveedores, colaboradores y demás partes interesadas.

Por tal razón, la organización se compromete a implementar, mantener y mejorar continuamente las medidas necesarias para proteger sus activos de información y gestionar los riesgos asociados al entorno digital, garantizando la confidencialidad, integridad, disponibilidad y privacidad de la información, en concordancia con la legislación colombiana vigente, las buenas prácticas internacionales y los lineamientos de Seguridad Digital promovidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

2. Objetivo

Establecer los principios, lineamientos y responsabilidades que permitan proteger los activos de información de ASISTENCIA SyS S.A.S., mediante la gestión integral de riesgos de seguridad de la información y seguridad digital, garantizando la continuidad de la operación y la confianza de las partes interesadas.

3. Alcance

La presente política aplica a:

- Todos los colaboradores, directivos, contratistas y terceros que tengan acceso a la información de la organización.
- Toda la información física y digital generada, procesada, almacenada, transmitida o custodiada por la empresa.
- Equipos de cómputo, dispositivos móviles, aplicaciones, redes, servicios en la nube, bases de datos, sistemas de información y demás activos tecnológicos.
- Procesos relacionados con la prestación de servicios de asistencia al hogar, asistencia legal y asistencia de transporte.

4. Principios de seguridad de la información

4.1 Confidencialidad

ASISTENCIA SyS S.A.S. garantizará que la información sea accesible únicamente para personas autorizadas, de acuerdo con sus funciones y responsabilidades.

Para ello:

- Se implementarán controles de acceso físico y lógico.
- Se protegerán los datos personales y la información sensible de clientes, proveedores y colaboradores.
- Se promoverá el uso adecuado de credenciales y mecanismos de autenticación.
- Se exigirán acuerdos de confidencialidad cuando corresponda.
- Se controlará el acceso a la información bajo el principio de mínimo privilegio.

4.2 Integridad

ASISTENCIA SyS S.A.S. garantizará que la información sea exacta, completa, confiable y protegida contra modificaciones no autorizadas.

Para ello:

- Se establecerán mecanismos de validación y control de cambios.
- Se mantendrá la trazabilidad de los registros críticos.
- Se protegerá la información contra alteraciones accidentales o intencionales.
- Se realizarán respaldos y controles que permitan la recuperación de la información.

4.3 Disponibilidad

ASISTENCIA SyS S.A.S. garantizará que la información, los sistemas y los servicios se encuentren disponibles cuando sean requeridos por los usuarios autorizados.

Para ello:

- Se realizarán copias de seguridad periódicas.
- Se implementarán mecanismos de recuperación ante incidentes.
- Se gestionarán los riesgos que puedan afectar la continuidad de los servicios.
- Se promoverá el mantenimiento preventivo y correctivo de la infraestructura tecnológica.
- Se definirán procedimientos para la gestión de incidentes de seguridad.

5. Gestión de riesgos de seguridad digital

La organización adoptará un enfoque basado en riesgos para identificar, analizar, evaluar, tratar y monitorear los riesgos que puedan afectar la seguridad de la información y la continuidad de la operación.

Todos los colaboradores deberán contribuir a la identificación y reporte oportuno de vulnerabilidades, amenazas e incidentes de seguridad.

6. Protección de datos personales

ASISTENCIA SyS S.A.S. protegerá los datos personales que recolecte, almacene o procese en desarrollo de sus actividades, dando cumplimiento a la Ley 1581 de 2012 y demás normas que la modifiquen o complementen.

La información personal será utilizada exclusivamente para los fines autorizados y bajo criterios de seguridad, confidencialidad y legalidad.

7. Gestión de incidentes de seguridad

Todo evento que comprometa o pueda comprometer la confidencialidad, integridad, disponibilidad o privacidad de la información deberá ser reportado inmediatamente a la persona o área responsable.

La organización establecerá procedimientos para:

- Identificación y reporte de incidentes.
- Contención y mitigación.
- Investigación y análisis de causas.
- Recuperación de servicios afectados.
- Implementación de acciones correctivas y preventivas.

8. Responsabilidades

Gerencia

- Aprobar la presente política.
- Proveer los recursos necesarios para su implementación.
- Promover una cultura organizacional orientada a la seguridad de la información.

Colaboradores y contratistas

- Cumplir los lineamientos establecidos en esta política.
- Proteger la información a la que tengan acceso.
- Reportar oportunamente incidentes o eventos sospechosos.
- Participar en actividades de sensibilización y capacitación.

Proveedores y terceros

- Cumplir los requisitos de seguridad definidos por la organización.
- Proteger la información entregada o administrada durante la prestación de sus servicios.

9. Concientización y cultura de seguridad

ASISTENCIA SyS S.A.S. publica esta política en su página web con el fin de fortalecer la cultura de seguridad de la información y promover el uso seguro de las tecnologías digitales.

10. Cumplimiento

El incumplimiento de esta política podrá dar lugar a la aplicación de medidas disciplinarias, contractuales o legales según corresponda.

11. Revisión y actualización

La presente Política de Seguridad de la Información entra en vigor a partir del 1 de diciembre de 2020, fecha de su aprobación por la Gerencia de Asistencia SyS S.A.S. y tendrá vigencia indefinida hasta que sea modificada, actualizada o sustituida por una nueva versión.

La política será revisada como mínimo una vez al año, o antes si se presentan cambios significativos en los procesos, servicios, infraestructura tecnológica, requisitos legales, riesgos de seguridad de la información o como resultado de incidentes que hagan necesaria su actualización.