Política de Seguridad de la Información

En Reportability, reconocemos que la información es un activo fundamental para nuestra operación, la confianza de nuestros clientes y el cumplimiento de nuestras obligaciones legales, éticas y contractuales, por ello esta Política de Seguridad de la Información establece los principios, responsabilidades y controles necesarios para proteger adecuadamente la confidencialidad, integridad y disponibilidad de la información gestionada por nuestra organización.

Entendiendo que la información es un activo fundamental para Reportability esta Política de Seguridad de la Información, tiene como objetivo proteger la confidencialidad, integridad y disponibilidad de los datos y sistemas, prevenir incidentes, y asegurar el cumplimiento de la normativa legal y contractual vigente.

1. Alcance

Esta política aplica a todos los colaboradores, consultores y terceros que tengan acceso a activos de información o sistemas tecnológicos de Reportability, ya sea directa o indirectamente.

2. Principios Generales

- Confidencialidad: acceso sólo por personas autorizadas.
- Integridad: la información debe mantenerse completa, exacta y sin modificaciones no autorizadas.
- Disponibilidad: acceso oportuno y confiable a la información cuando sea requerido.

3. Lineamientos de Seguridad de la Información

Para cumplir con los principios anteriores, se establecen los siguientes lineamientos:

- Contar con una Política de Seguridad de la Información aprobada por la dirección y difundida entre todos los colaboradores.
- Implementar un Plan de Concientización y Capacitación en Seguridad de la Información (SI), con actividades periódicas.
- Establecer y mantener normas, procesos o procedimientos documentados para:

- **Gestión de accesos:** Definición y control de permisos de acceso a la información y sistemas, de acuerdo al principio de mínimo privilegio.
- **Gestión de vulnerabilidades:** Identificación, análisis y corrección de debilidades técnicas mediante revisiones periódicas y escaneos de seguridad.
- **Gestión de parches de seguridad:** Aplicación oportuna de actualizaciones de software para reducir el riesgo de explotación de fallas conocidas.
- **Gestión de respaldos:** Ejecución periódica de copias de seguridad, almacenadas de forma segura, con pruebas de restauración documentadas.
- **Gestión de cambios:** Registro y autorización formal de modificaciones en sistemas, infraestructura o configuraciones tecnológicas.
- **Gestión de monitoreo:** Supervisión continua de la actividad de los sistemas críticos para detectar accesos no autorizados o comportamientos anómalos.
- **Gestión de incidentes:** Definición de procedimientos para notificar, contener, investigar y resolver eventos de seguridad, con responsables definidos.
- Definir el estándar de endurecimiento de estaciones de trabajo, incluyendo configuración segura, restricción de puertos, y uso obligatorio de antivirus.

4. Responsabilidades

La alta dirección es responsable de aprobar y respaldar esta política. El responsable de tecnologías de la información deberá coordinar su implementación. Cada colaborador debe cumplir con los lineamientos definidos, participar en actividades de capacitación y reportar cualquier incidente o situación anómala.

5. Cumplimiento y Actualización

El incumplimiento de esta política podrá dar lugar a responsabilidades contractuales, según la normativa laboral vigente. Esta política será revisada anualmente o cuando ocurran cambios relevantes en los sistemas, procesos o riesgos de seguridad.

Powered by ecert
Firma electrónica avanzada
CARLA LORENA HORTA DEL PICO
2025.08.23 15:37:45 -0400

Carla Horta del P.

Gerente general

Reportability