STOREY S.A.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Dirección de STOREY S.A entiende que la información tiene un valor fundamental para la organización y por consiguiente debe ser debidamente protegida. Por ello, promueve y se compromete con la mejora continua del Sistema de seguridad de la información y a satisfacer sus requisitos mediante la formulación y el mantenimiento de una política adecuada que proporcione un marco de trabajo para establecer los objetivos de seguridad de la información.

El presente documento se aprueba por la Dirección de STOREY S.A quien se compromete a publicarlo y comunicarlo, y a exigir su cumplimiento a todo el personal de la compañía y a los terceros que interactúan de manera habitual u ocasional que puedan acceder a información sensible.

La Política de Seguridad de la Información de STOREY S.A se encuentra basada en los siguientes ejes estratégicos:

- **Organización de la Gestión de Seguridad de la Información**: orientada a definir roles y responsabilidades de acuerdo con las diferentes funciones que se desprendan de la gestión de la seguridad de la información, estableciendo el marco de trabajo para la gestión del riesgo y delineando las condiciones y requisitos de seguridad para terceros que tengan accesos a información e instalaciones de procesamiento de la misma.

- **Clasificación y Control de la información:** orientado a definir pautas generales para asegurar una adecuada clasificación, tratamiento y control de la información teniendo en cuenta los criterios de confidencialidad, integridad y disponibilidad de la información.

- **Concientización del Personal:** orientada a poner en conocimiento a empleados y terceros acerca del contenido de la presente política como así también los procesos disciplinarios que deriven de su cumplimiento, logrando crear conciencia del buen uso de los recursos informáticos de la compañía.

- **Seguridad Física y Ambiental:** orientada a realizar controles sobre la eficacia de las medidas de protección físicas implementadas para proteger instalaciones y equipos de procesamiento de información contra amenazas físicas, lógicas y/o ambientales que podrían afectar la seguridad de la información.

- **Gestión de comunicaciones y operaciones:** orientada a asegurar una correcta operación de las instalaciones de procesamiento de información, la integridad de las aplicaciones y la confidencialidad de las comunicaciones, estableciendo controles técnicos y procedimientos.

- **Control de acceso a los sistemas de información:** orientado a controlar el acceso a la información y a los sistemas que la procesan en base a los requisitos del negocio y de la seguridad; los cuales solo son concedidos de acuerdo con la necesidad de conocimiento, previniendo a través de controles técnicos apropiados los accesos no autorizados a los sistemas de información.

- **Desarrollo y mantenimiento de los sistemas:** orientado a procurar un entorno de desarrollo seguro que cumpla con requisitos de seguridad en todas sus fases.

- **Gestión de la continuidad del negocio:** orientada a desarrollar controles sobre los planes de recuperación ante desastres y de continuidad del negocio para garantizar el normal funcionamiento de la compañía y ambientes de tecnología ante una contingencia.

- **Gestión de incidentes de seguridad de la información:** orientada a reducir al mínimo el daño causado por los mismos, permitiendo el monitoreo y desarrollo de una base de conocimiento.

  Gestión de Activos Críticos de Conocimiento: orientado a establecer un proceso para identificar y clasificar los activos de información que contienen conocimiento crítico para el negocio. Esto podría incluir datos financieros, estrategias comerciales, propiedad intelectual, datos de clientes clave y conocimientos adquiridos por los recursos humanos.

- **Integración de Conocimiento del Negocio en Procesos de RRHH:** integrar el conocimiento del negocio en los procesos de recursos humanos, como la selección y contratación, la formación y el desarrollo, la evaluación del desempeño y la planificación de la sucesión. Esto asegurará que los empleados de STOREY tengan en cuenta las necesidades específicas del negocio al tomar decisiones y brindar apoyo a los demás empleados.

JUAN FERNÁNDEZ

Gerente I+D

abril 2024