POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN

1. Introducción

Este documento establece la política de Colinet Trotta basada en la Norma ISO 27001.

Colinet Trotta es una empresa de tecnología dedicada a la:

“Comercialización, análisis, diseño, desarrollo, testing, implementación, consultoría y mantenimiento posventa de sistemas de gestión para compañías de seguros y afines.

Comercialización de hardware y software de terceros.

Comercialización y prestación de servicios de computación en la nube”.

Colinet Trotta se compromete a garantizar la confidencialidad, integridad y disponibilidad de la información en todas las áreas de la organización. Para ello establece un Sistema de Gestión de Seguridad de la Información a través de un conjunto de medidas integrales y controles de seguridad para la protección de los activos y datos sensibles de la empresa y sus clientes, asegurando la continuidad del negocio y la preservación de la información.

Colinet Trotta se compromete a la mejora continua de su SGSI, así como a cumplir con los requisitos legales y regulatorios pertinentes y de sus partes interesadas en materia de seguridad de la información.

2. Alcance

Esta política se aplica a todos los empleados, contratistas, proveedores y a cualquier otra parte que tenga acceso a los sistemas y datos de Colinet Trotta.

Colinet Trotta será estricto en el cumplimiento de las políticas de seguridad establecidas por sus clientes para con la información accesible así como de sus partes interesadas.

Se aplica a todos los activos de información, ya sea en formato electrónico, impreso o cualquier otro medio.

Esto abarca a todos los activos de información relacionados con el desarrollo, mantenimiento, implementación y soporte de soluciones de software, así como a la administración y ejecución de las operaciones de la empresa, incluyendo a su infraestructura tecnológica y sistemas de gestión internos.

Los procesos alcanzados se encuentran definidos en el Manual - Sistema de Gestión Integral.

3. Responsabilidades

La dirección es responsable de garantizar que se asignen recursos adecuados para implementar y mantener medidas de seguridad. Como así también de garantizar que sean establecidos los objetivos y planes para el SGSI y que estos sean revisados, al menos, de forma anual.

El Responsable de Seguridad de la Información (RSI) se ocupa de supervisar la aplicación de las políticas, procedimientos y controles, así como de definir y diseñar los controles en apoyo a los propietarios de los activos.

Los responsables de área serán los propietarios de los activos y del riesgo de los mismos, así como de la definición e implementación de sus controles con el apoyo del RSI.

Todos los empleados son responsables de adherirse a esta política y de contribuir a la seguridad de la información por lo que deben ser conscientes de los riesgos de seguridad de la información dentro de sus actividades diarias en la empresa.

4. Desarrollo de la política

4.1 Control de la información y control de los accesos

Se establecen niveles de clasificación de la información para determinar los niveles de acceso y protección requeridos con el fin de prevenir la divulgación, modificación, eliminación o destrucción no autorizados de información almacenada en medios.

Acceso y control de la información:

Se asignan permisos de acceso basados en el principio de "menos privilegios". Se implementa un sistema de gestión de identidad y acceso para administrar la autorización de usuarios.

Se establecen controles para garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles.

4.2 Controles criptográficos

Colinet Trotta garantiza el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

4.3 Seguridad de las operaciones

En Colinet Trotta:

- Garantizamos la operación correcta y segura de las instalaciones de procesamiento de la información.
- Garantizamos que la información y las instalaciones de procesamiento de información estén protegidas contra código malicioso y otras vulnerabilidades técnicas.
- Nos protegemos contra la pérdida de datos.
- Registramos eventos y generamos evidencia en nuestro sistema de trackeo.
- Garantizamos la integridad de los sistemas en producción.

4.4 Seguridad de las comunicaciones

Garantizamos la protección de la información en las redes y sus instalaciones de procesamiento de la información que la soportan.

4.5 Adquisición, desarrollo y mantenimiento de los sistemas

Garantizamos que la seguridad de la información sea una parte integral de los sistemas de información a lo largo de todo el ciclo de vida, también que se diseñe e implemente en forma temprana el desarrollo de los sistemas de información con la activa participación del RSI en los proyectos.

4.6 Relación con los proveedores

Garantizamos la protección de los activos de la organización a los cuales tienen acceso los proveedores, manteniendo un nivel acordado de seguridad de la información y de prestación de servicios, alineados con los acuerdos con los proveedores.

4.7 Desarrollo de software seguro

Se siguen prácticas de desarrollo seguro, como revisión de código, pruebas de seguridad y evaluaciones de vulnerabilidades.

Se mantienen actualizados los componentes y bibliotecas de software utilizados.

4.8 Seguridad en la infraestructura

Los sistemas críticos se alojan en entornos seguros y se aplican actualizaciones regularmente.

4.9 Respuesta a incidentes

Se mantiene un plan de respuesta a incidentes que incluya procedimientos para detectar, informar y mitigar incidentes de seguridad.

Los incidentes se documentan y se realizan análisis post-incidentes para mejorar la seguridad.

4.10 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

Consideramos la continuidad de la seguridad de la información en los sistemas de gestión de la continuidad del negocio de Colinet Trotta, garantizando la disponibilidad de las instalaciones de procesamiento de la información.

4.11 Formación y concientización

Se llevan a cabo programas regulares de formación en seguridad para empleados y contratistas para garantizar que todos comprendan sus responsabilidades y estén al tanto de las amenazas y mejores prácticas, para así garantizar que las personas que realizan el trabajo bajo el control de la organización entiendan sus responsabilidades y sean idóneos para los roles para los cuales se las considera.

Se promueve la concientización sobre seguridad de la información a través de campañas de sensibilización y capacitación.

4.12 Cumplimiento legal y normativo

La empresa cumple con las leyes y regulaciones de protección de datos y seguridad de la información aplicables.

Se establecen procedimientos para garantizar el cumplimiento de estándares relevantes (ISO 27001 aplicable).

5. Revisión de la Política

Esta política se revisará, al menos, anualmente para garantizar su relevancia y eficacia en un entorno en constante evolución.

La mejora continua es un pilar fundamental para mantener y actualizar el SGSI de acuerdo con las cambiantes amenazas y requisitos de seguridad.

6. Documentos relacionados

El documento de aplicabilidad explica la aplicación de cada control al SGSI.

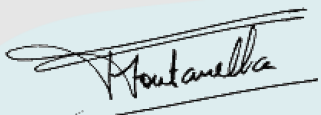
7. Aprobación y divulgación

Todos los empleados, contratistas y terceros deben leer, comprender y aceptar esta política antes de interactuar con los sistemas y la información de Colinet Trotta.

Directorio Colinet Trotta

Vigencia: 15/10/23

Versión 01



Fabio Fontanella
Director y Vicepresidente
COLINET TROTTA S.A.