Política de Seguridad de la Información

Objeto

Establecer las directrices y principios que regirán el modo en que Grant Thornton gestionará y protegerá su información y sus servicios, a través de la implantación, mantenimiento y mejora de un **Sistema de Gestión de Seguridad de la Información** (en adelante, SGSI) en base a los requisitos de la norma ISO/IEC 27001 y de sus partes interesadas, dentro del marco regulatorio legal y vigente.

Alcance

Tomando en cuenta el contexto de Grant Thornton para el SGSI, en el cual se determinan las cuestiones internas y externas de la Firma, las partes interesadas que son relevantes y sus requisitos para la seguridad de la información, así como las interfaces y dependencias entre las actividades realizadas por la Firma y las que se llevan a cabo por otras organizaciones en el cumplimiento de su misión como entidad privada.

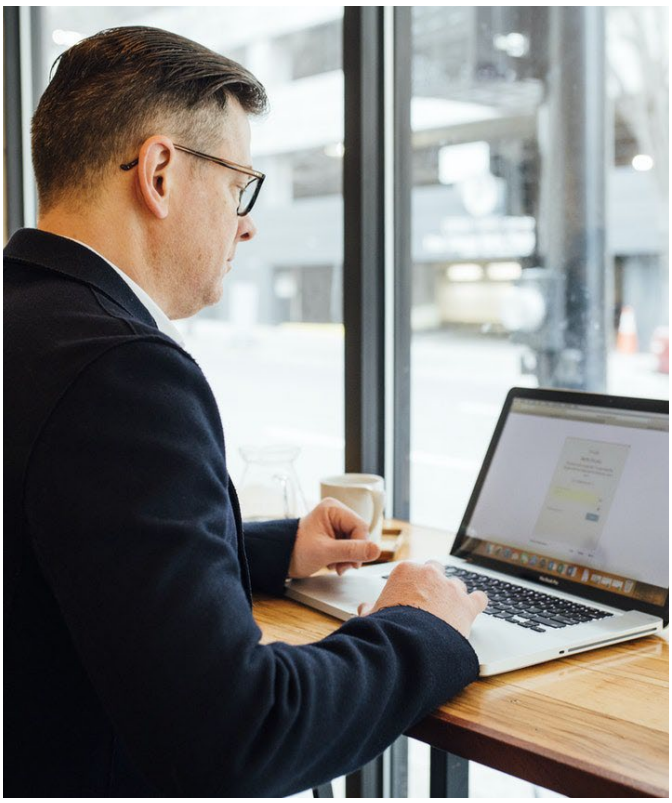
Misión

Con el SGSI, se fortalece la seguridad de los servicios, así como de la información y datos que incluyen dichos servicios y que son necesarios para su correcta y adecuada prestación, por la estrecha relación entre ambos y los elementos adicionales que mejoran notablemente la gestión de la seguridad que es necesaria para Grant Thornton.

Marco legal y regulatorio

La presente política y el SGSI se mantendrá en concordancia con el marco legal vigente siendo necesario una revisión continua del mismo.

Grant Thornton trata los datos de carácter personal bajo la responsabilidad de las entidades correspondientes de la red Grant Thornton International Ltd. y con las medidas de seguridad aplicables de acuerdo a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de



los derechos digitales así como las instrucciones de los organismos competentes en materia de protección de datos personales.

Establecer procedimientos para cumplir la Ley de Propiedad Intelectual (Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia).

Dentro del proceso de digitalización de los procesos y servicios cumplirá con la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Ley 1/2019, de 20 de febrero, de Secretos Empresariales, con el objetivo de proteger la información empresarial no divulgada (secretos empresariales) de Grant Thornton.

Liderazgo y compromiso

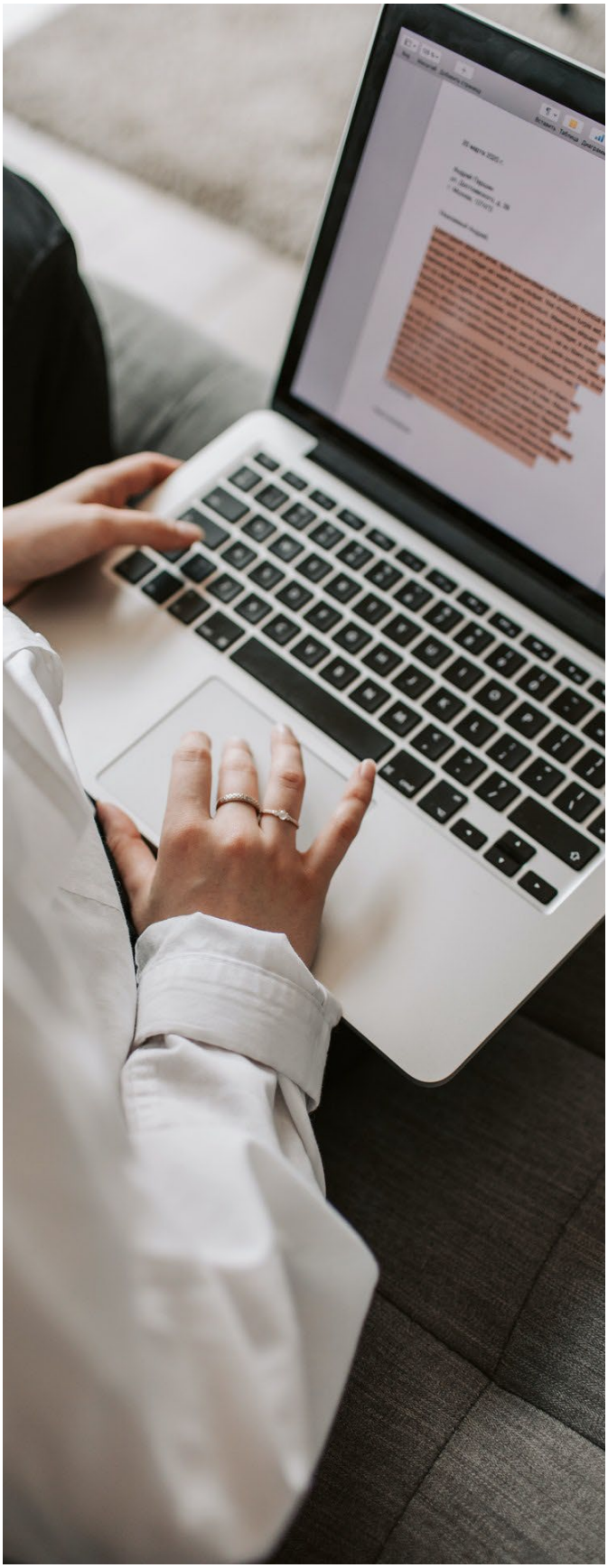
La Dirección de Grant Thornton se compromete a facilitar y proporcionar los recursos necesarios para el establecimiento, mantenimiento y mejora del SGSI de la Firma, así como a demostrar liderazgo y compromiso respecto a este, a través de la constitución del Comité de Seguridad que tendrá la responsabilidad de:

- Asegurar el establecimiento de la presente política y los objetivos de la seguridad de la información, y que estos sean compatibles con la estrategia de Grant Thornton.
- Asegurar la integración y el cumplimiento de los requisitos aplicables del SGSI en los procesos de la Firma.
- Asegurar que los recursos necesarios para el SGSI estén disponibles.
- Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del SGSI.
- Asegurar que el SGSI consigue los resultados previstos.
- Dirigir y apoyar a las personas para contribuir a la eficacia del SGSI.
- Promover la mejora continua.
- Apoyar otros roles pertinentes de la Dirección, liderando a sus áreas de responsabilidad en seguridad de la información.
- Indicadores para evaluar el resultado y cumplimiento.

Objetivos

Los objetivos de seguridad de la información se establecerán en las funciones y niveles pertinentes, enfocados a la mejora y utilizando como marco de referencia:

- Cambios en las necesidades de las partes interesadas que lleven a una mejora del alcance.
- Requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información.
- Factores internos como la aplicación de técnicas organizativas que mejoren el seguimiento de la tramitación y resolución de incidentes de seguridad.
- Factores externos como clientes y los avances tecnológicos, cuya aplicación mejoren la eficacia del tratamiento de los riesgos.
- La mejora de la eficacia de la formación y concienciación del personal que trabaja en la Firma y afecta a su desempeño en seguridad de la información.



Mejora continua

Grant Thornton determinará el nivel de riesgo de seguridad de la información en que se encuentra la Firma e identificará los controles de seguridad necesarios para el tratamiento del riesgo y llevarlo a un nivel aceptable, así como las oportunidades de mejora, considerando las cuestiones internas y externas y los requisitos de las partes interesadas antes indicados.

Los controles de seguridad deberán implantarse, mantenerse y mejorarse continuamente, y estar disponibles como información documentada, revisada y aprobada por el Comité Seguridad.

Se deberá comunicar la información documentada de los controles de seguridad al personal que trabaja en la Firma (empleados y proveedores), que tendrá la obligación de aplicarla en la realización de sus actividades laborales, comprometiéndose de ese modo, al cumplimiento de los requisitos del SGSI.

La información documentada será clasificada en: pública, interna y confidencial, dando el uso adecuado de acuerdo a dicha clasificación y según el criterio que se establezca en el procedimiento de clasificación, etiquetado y protección de la información.

Se realizarán auditorías que revisen y verifiquen el cumplimiento del SGSI, por lo que, en caso necesario, el personal afectado por el alcance deberá colaborar en estas para una mejora continua.

Si necesitara cualquier información adicional sobre la Política de Seguridad de la Información o tiene alguna sugerencia al respecto puede enviar un mensaje de correo electrónico a la siguiente dirección: sgsi@.es.gt.com

Funciones y/o responsabilidades

El Comité de Seguridad será el órgano encargado de aprobar la política y será el responsable de la autorización de sus modificaciones, así como de toda la información documentada del SGSI.

El Responsable de Seguridad será el encargado de notificar la presente política al personal de Grant Thornton, y proveedores, y de los cambios que en ella se produzcan, así como de coordinar las acciones de implantación, mantenimiento y mejora del SGSI de la Firma, y de sus auditorías.

El Delegado de Protección de Datos será el responsable de supervisar y velar por el cumplimiento de la normativa vigente en materia de protección de datos personales.

Todo el personal de la Firma será responsable de cumplir la presente política dentro de su área de trabajo, así como de aplicar toda la información documentada del SGSI en sus actividades laborales que afecta a su desempeño en seguridad de la información.

Revisión

La presente Política de Seguridad de la Información será examinada en las revisiones del SGSI por la Dirección, a través del Comité de Seguridad, siempre que se produzcan cambios significativos, como mínimo, una vez al año.

Aprobación, difusión y aplicación

La presente Política de Seguridad de la Información es aprobada por el Comité de Seguridad de Grant Thornton y difundida a las partes interesadas de la Firma, con fecha de aprobación a 4 de diciembre de 2020. Así mismo, la Dirección de Grant Thornton dotará de los recursos necesarios para la aplicación efectiva de esta política, y para su buen desarrollo, tanto en las actividades de implantación como en su posterior mantenimiento y mejora de todo el SGSI de la Firma.