Política corporativa 7

Seguridad global de la información y sistemas

Finalidad

La finalidad de esta Política es establecer el compromiso de Stryker de adecuar los controles de seguridad en su información, sistemas y operaciones para que estén conformes con la legislación aplicable.

Alcance

Esta Política se aplica a todos los empleados y terceros de Stryker (p. ej., proveedores, contratistas, agentes) que actúen en nombre de Stryker, independientemente de su ubicación. Si cualquier disposición de esta Política no cumple con la ley local o regional aplicable para una entidad jurídica específica de Stryker, dicha entidad implementará, en la medida necesaria, un apéndice a esta Política para cumplir con la ley local o regional, siempre que la política revisada se ajuste en la mayor medida posible a los principios contenidos en esta Política. Dicho apéndice deberá ser aprobado por el CISO. Cuando no se haya implementado un apéndice local o regional, todas las disposiciones de esta Política permanecerán vigentes en la medida que cumplan con la legislación aplicable.

Políticas básicas

Stryker cumplirá con todas las leyes que rigen la seguridad de los sistemas y productos de Stryker. Además, Stryker está comprometida con los estándares que se exponen a continuación.

1. **Designar un director ejecutivo de seguridad de la información ("chief information security officer", CISO):** El CISO es responsable de establecer y hacer cumplir el funcionamiento efectivo del programa de seguridad global de la información de Stryker y alinear las iniciativas de seguridad con los programas empresariales y objetivos comerciales para la protección de las tecnologías, sistemas, productos y activos de información.

2. **Implementar políticas de seguridad y estructuras administrativas y de gobierno:** Stryker implementará, a través de los sistemas de gestión de la calidad, el sistema de gestión de seguridad de la información, los estándares de gobierno de la información, los estándares de uso aceptable, el plan de respuesta ante incidentes y los procedimientos y normas pertinentes relacionados, los controles de seguridad físicos, técnicos y administrativos apropiados.

3. **Evaluar a terceros:** Debe completarse el proceso de evaluación de la seguridad global antes de contratar a cualquier tercero que tenga acceso a las redes de Stryker o a datos sensibles en formato electrónico o que proporcione software o soluciones basadas en Internet para uso interno o para usar en una oferta de productos o servicios de Stryker.

4. **Utilizar sistemas y equipos de Stryker:** Cualquier empleado de Stryker o tercero que tenga acceso a los sistemas o equipos de Stryker utilizará tales equipos y sistemas de acuerdo con los requisitos pertinentes de uso aceptable.

Responsabilidades

Es responsabilidad de todos los empleados de Stryker y terceros cumplir con esta Política y todos los procedimientos y normas de implementación pertinentes. El CISO, en coordinación con las funciones y unidades de negocio aplicables, identificará cualquier procedimiento y norma adicional necesarios para cumplir con esta Política y preparará e implementará dichos procedimientos y normas.

Cumplimiento

Stryker requiere que todos los empleados y terceros cumplan con esta Política. Si tiene alguna pregunta sobre esta Política o los procedimientos relacionados o alguna inquietud relacionada con el programa de seguridad de Stryker, póngase en contacto con el representante local de Recursos Humanos de Stryker, el responsable de cumplimiento, el asesor jurídico o la Línea directa para temas de Ética. Stryker mantendrá la confidencialidad de tales preguntas o inquietudes de conformidad con los procedimientos y políticas de la Línea directa para temas de Ética.