

POLÍTICA DE CIBERSEGURIDAD DEL GRUPO SCHILLER

Compromiso con la ciberseguridad

SEGURIDAD DE LA INFORMACIÓN

SCHILLER está comprometida con la ciberseguridad:

- ❖ Nuestro objetivo es cumplir la norma ISO 27001 y otros requisitos aplicables relacionados con la seguridad de la información, gestionando y mitigando con eficacia los riesgos de ciberseguridad en todas nuestras operaciones.
- ❖ Nos comprometemos a cumplir nuestras obligaciones de conformidad con la norma.
- ❖ Nuestras medidas tienen por objeto garantizar la protección de la información personal y de la ePHI de conformidad con la legislación aplicable en materia de privacidad.
- ❖ Nos aseguramos de que la ciberseguridad se incorpore plenamente a nuestros procesos comerciales, manteniendo nuestro compromiso tanto con la ciberseguridad como con la gestión de la calidad.
- ❖ Nos fijamos objetivos compatibles con la dirección estratégica y el contexto de nuestra organización.
- ❖ Al proteger los secretos comerciales y la información sujeta a derecho de propiedad contra el acceso y la divulgación no autorizados, reforzamos nuestra dedicación al suministro de dispositivos y servicios médicos de la máxima calidad.

MEJORA CONTINUA

SCHILLER se esfuerza por mejorar continuamente la seguridad de la información

- Nuestro compromiso incluye evaluaciones periódicas de los riesgos y la adopción de controles técnicos y organizativos adecuados para gestionar los riesgos de ciberseguridad.
- Realizamos auditorías y revisiones para evaluar de forma continua la idoneidad, adecuación y eficacia de las medidas de ciberseguridad.
- Determinamos cuáles son las oportunidades de mejora y garantizamos la disponibilidad de los recursos necesarios.
- Integramos sólidas prácticas de ciberseguridad en nuestro sistema de gestión de calidad para mantener los más altos estándares de nuestros productos y servicios.

CONCIENCIACIÓN DE LOS EMPLEADOS

SCHILLER informa y proporciona formación a sus empleados sobre ciberseguridad

- Nos comprometemos a salvaguardar la integridad, confidencialidad y disponibilidad de los activos de información, que abarcan los procesos de producción, la infraestructura de TIC, la información personal, la información sanitaria electrónica protegida (ePHI) y los secretos comerciales.
- Comunicamos esta política a nuestros empleados.
- Nos aseguramos de que los empleados sean conscientes de los riesgos de ciberseguridad y de las ventajas de gestionarlos y mitigarlos eficazmente en todas nuestras operaciones.
- Nuestros empleados comprenden la importancia de la ciberseguridad y cumplen los requisitos aplicables.