POLÍTICA DE CIBERSEGURIDAD

El marco de CIBERSEGURIDAD contiene las normas y regulaciones que establecen los requisitos organizativos, de procedimiento y técnicos para proteger los activos de información y los productos y soluciones de ALPASA frente a las ciberamenazas internas y externas, mejorando la capacidad de resiliencia de los negocios.

ALPASA considera la información como uno de sus activos más importantes para el correcto y eficiente desarrollo de sus servicios y el cumplimiento de los objetivos y leyes, estableciendo así la seguridad de la información como objetivo fundamental para garantizar que la información procesada sea precisa, está disponible a quién la requiera y no se revele sin autorización.

ALPASA considera la serie ISO / IEC 27000 como estándar para este marco general.

ALPASA es consciente de la evolución asociada a las ciberamenazas y las regulaciones de la Tecnología de Operación (OT) y Sistemas de Control Industrial (ICS), estableciendo la Seguridad en Productos y Soluciones como objetivo fundamental para garantizar que las infraestructuras críticas que soportan los productos y servicios de la compañía están protegidas.

ALPASA considera la serie IEC 62443 como estándar para este marco general.

PRINCIPIOS BÁSICOS

La política de ciberseguridad se basa en los siguientes principios básicos:

• Garantizar que los sistemas de información (IT) y sistemas de operación (OT) de la compañía tengan un nivel de seguridad y resiliencia adecuado y apliquen los estándares más avanzados en los activos tecnológicos que respaldan la operación de infraestructuras críticas.

• Implementar las medidas de seguridad necesarias para proteger la confidencialidad, la integridad y la disponibilidad de la información y los sistemas de operación en función de su criticidad y los riesgos existentes, siguiendo un enfoque basado en el riesgo.

• Promover la implantación de mecanismos de seguridad y resiliencia adecuados para los sistemas y operaciones gestionados por terceros que prestan servicios a la compañía.

• Sensibilizar a todos los empleados, contratistas y colaboradores sobre los riesgos de ciberseguridad y garantizar que tengan los conocimientos, habilidades, experiencia y capacidades tecnológicas necesarios para respaldar los objetivos de la compañía.

• Promover las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación contra incidentes y actividades del cibercrimen.

• Proporcionar procedimientos y herramientas para adaptarse rápidamente a las condiciones cambiantes del entorno tecnológico y las nuevas amenazas.

• Garantizar el cumplimiento normativo asociado a las áreas de ciberseguridad en toda la compañía.

• Colaborar con organizaciones, agencias gubernamentales y asociaciones relevantes para contribuir a la mejora global de la ciberseguridad.

JORGE FERNANDEZ WILBURN
DIRECTOR GENERAL GRUPO DPH

REV. 01 20/05/2020