POLÍTICA DE CIBERSEGURIDAD

Objetivo y Alcance

Esta política establece las normas para proteger la confidencialidad, integridad y disponibilidad de la información.
Alcance: Aplica a todo el personal, colaboradores y terceros con acceso a los sistemas (ERP, Email, Plataformas de Documentación).
Marco Legal: Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD). Ley de Ciberresiliencia de la UE

Control de Acceso y Gestión de Identidad

Dado el uso de ERP y aplicaciones de clientes, se implementa un modelo de Confianza Cero (Zero Trust):
Autenticación: Uso obligatorio de Factor de Autenticación (Usuario y Contraseña) para acceso al ERP.
Contraseñas: Deben ser únicas, complejas y gestionadas preferiblemente a través de un gestor de contraseñas corporativo.
Principio de Privilegio Mínimo: Los usuarios solo tendrán acceso a la documentación y funciones del ERP estrictamente necesarias para su puesto mediante sistema de roles en el perfil de cada usuario.

Seguridad en el Correo Electrónico y Comunicaciones

Uso Profesional: El correo corporativo se usará exclusivamente para fines laborales.
Prevención de Phishing: Prohibición de abrir enlaces o descargar archivos de remitentes desconocidos sin verificar su autenticidad.
Cifrado: Los correos que contengan datos sensibles o protegidos por el RGPD deben enviarse cifrados.

Gestión de Documentación y Datos

Plataformas Autorizadas: Queda prohibido el uso de nubes personales (ej. Dropbox personal) para mover datos de la empresa.
Clasificación de Información: La documentación se etiquetará según su sensibilidad (Pública, Interna, Confidencial).
Limpieza de Datos: Eliminación periódica de documentos que hayan cumplido su propósito o plazo legal de conservación.

Seguridad en ERP y Aplicaciones de Clientes

Actualizaciones: El software debe mantenerse siempre en su última versión para parchear vulnerabilidades.
Auditoría de Logs: Se registrarán los accesos y modificaciones en el ERP para garantizar la trazabilidad de los datos de los clientes.
Entornos Seguros: Las aplicaciones de clientes deben seguir los estándares de la Ley de Ciberresiliencia de la UE.

Continuidad de Negocio y Respuesta a Incidentes

Copias de Seguridad (Backup): Realización de backups diarios automatizados y almacenados de forma aislada (regla 3-2-1).
Notificación de Brechas: Cualquier incidente de seguridad debe reportarse al Responsable de Seguridad inmediatamente. Si hay afectación de datos personales, la empresa debe notificar a la AEPD en un plazo máximo de 72 horas.

Formación y Concienciación

Todo el personal recibirá una sesión de formación anual sobre amenazas actuales y buenas prácticas digitales.

Román Bono Torres

Gustavo Paulo Duarte