El Grupo VILOR, formado por las empresas VILOR INFRAESTRUCTURAS, S.L. y ACTIVIDADES DE INFRAESTRUCTURAS PÚBLICAS Y CONSERVACIÓN, S.L., VILOR CARRETERAS Y FIRMES, S.L.U., VILOR AGUA Y MEDIOAMBIENTE, S.L.U. y VILOR INSTALACIONES, S.L.U., liderado por la constructora valenciana VILOR INFRAESTRUCTURAS, S.L., es un grupo de empresas dedicadas al sector de la construcción, instalaciones, servicios de conservación y mantenimiento de infraestructuras, tanto públicas como privadas, que ofrece soluciones a las necesidades actuales del mercado, a través de cada una de sus empresas y tiene, como parte de sus objetivos, el de garantizar la seguridad de la información, de manera preventiva y continuada, antes, durante y tras la prestación de los servicios.

Los objetivos del Grupo VILOR, en materia de seguridad de la información, son:

- Garantizar la autenticidad, confidencialidad, integridad, acceso, disponibilidad, trazabilidad y conservación de los datos, información y servicios utilizados por medios electrónicos, manteniendo la estrategia de adaptación a los cambios en las condiciones del entorno.
- Cumplir la legislación y regulación aplicable, estableciendo como marco legal y regulatorio básico el Esquema Nacional de Seguridad (ENS) en el que basan los mecanismos (preventivos, de control y detección, correctivos y de reposición) establecidos e implementados por esta organización, para garantizar que el sistema de seguridad de la información del Grupo VILOR permite asegurar la categoría de seguridad ALTA.
- Establecer responsabilidades claras para la gestión de la seguridad de la información.
- Garantizar la calidad, robustez, resiliencia y capacidad de detección y respuesta del sistema de seguridad de la información, basado en el análisis y gestión de los riesgos, para minimizar el impacto sobre el sistema de seguridad de la información en caso de producirse ante amenazas, incidentes de seguridad y otras contingencias de importancia para la integridad del sistema.
- Asegurar la recuperación y reposición rápida y eficaz de los servicios afectados por cualquier tipo de contingencia que pudiera poner en riesgo la continuidad de las actividades de la organización, de cualquier tipo de requisitos legal y suscrito, así como demás compromisos adquiridos con los clientes.
- Fomentar la cultura de seguridad de la información en el seno de toda la organización.

El marco regulatorio más relevante, en el que nos apoyamos para establecer la Política ENS del Grupo VILOR, es entre otros, el siguiente:

- Esquema Nacional de Seguridad (ENS): RD 311/2022, de 3 de Mayo.
- Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPD): Ley Orgánica 3/2018, de 5 de diciembre.
- Reglamento general de protección de datos (RGPD): Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril.
- Procedimiento Administrativo Común de las Administraciones Públicas (PACDP): Ley 39/2015, de 1 de octubre.
- Régimen Jurídico del Sector Público (RJSP): Ley 40/2015, de 1 de octubre.
- Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI).
- Ley de Propiedad Intelectual (LPI): RD-Legislativo 1/1996, de 12 de abril, y modificaciones posteriores.

Estructura y composición del Comité de Seguridad de la información: El Comité para la gestión y coordinación de la seguridad de la información, es el órgano con mayor responsabilidad, dentro del sistema de gestión de seguridad de la información, y el que acuerda las decisiones más importantes relacionadas en esta área.

El procedimiento para la designación y renovación de sus miembros, así como el establecimiento de los mecanismos de coordinación y resolución de posibles conflictos, dentro de las atribuciones de los diferentes responsables, será mediante reunión del propio Comité de seguridad y ratificación en su Acta correspondiente.

Los roles o funciones de seguridad principales, definidos para cada figura del Comité de Seguridad de la Información del Grupo VILOR, son:

- **Dirección:** Liderar el sistema de seguridad de la información, basado en el ENS, y proporcionar los recursos necesarios para su implantación, desarrollo y mantenimiento.
- **Responsable de la Información (Jefe TIC)**: Establecer los requisitos y/o niveles de seguridad de la información tratada, en materia de seguridad de la información, según los parámetros del Anexo I del ENS.
- **Responsable del Servicio (Jefe TIC):** Coordinar la implantación y mejora continua del sistema de seguridad de la información.
- **Responsable de Seguridad (Jefe TIC):** Determinar las necesidades y decisiones de seguridad pertinentes para satisfacer los requisitos e idoneidad de las medidas técnicas establecidas, la tecnología idónea para el servicio y promover la formación y concienciación en este ámbito.
- **Responsable del Sistema (Técnico/a Informático/a):** Coordinar la implantación, desarrollar, operar, mantener, analizar los riesgos e incidentes, establecer planes de contingencia, verificar, y promover la mejora continua del sistema de seguridad de la información.
- **Delegado de Protección de Datos (Jefe de Administración):** Velar por el cumplimiento del Reglamento de desarrollo de la LOPD, en virtud de los artículos 109 y 95 del RGPD que desarrolla la LOPD.
- **Plantilla del Grupo VILOR**, al completo: Responsables de informar sobre las debilidades e incidentes de seguridad de la información que se detecten, durante el desarrollo de actividad.

Estructura de la gestión y acceso documental, del sistema de seguridad de la información: El Grupo VILOR garantiza la integridad del sistema de seguridad de la información, durante todo el ciclo de vida de sus actividades y procesos, desde la concepción del sistema hasta su retirada, mediante:

- La organización e implantación del sistema de seguridad de la información, con sus procesos de seguridad y con garantías de protección adecuadas al nivel de seguridad ALTO, tanto en las instalaciones, como la estructura, equipamiento y repositorio documental.
- El análisis y gestión de los riesgos, con la implantación de mecanismos y elementos de seguridad adecuados al resultado de la evaluación y análisis de los riesgos y amenazas, previo, con metodología reconocida, basada en la metodología ***Magerit***, y con periodicidad anual, cuando se produzcan incidentes o vulnerabilidades graves sobre la seguridad y/o cuando sucedan cambios significativos en los servicios prestados e información manejada.
- La gestión del personal y su profesionalidad, capacitando al personal de la organización a través de la formación, información y concienciación continua, en esta materia y con frecuencia mínima anual y, especialmente, capacitando al personal cualificado del Grupo VILOR, con responsabilidad directa en la gestión del sistema de seguridad, previa a la asunción de sus responsabilidades en esta área, a través de la formación continua y específica en el sistema de seguridad de la información y sus deberes y responsabilidades, así como de su evaluación del desempeño.
- La autorización y control de los accesos, con la implantación de técnicas de autenticación, de autorización y estricto control de acceso y de conexiones para la protección de las redes y los elementos críticos del sistema, para mantener la restricción del acceso sólo al personal previsto y autorizado, así como formación y concienciación a toda la plantilla, sobre el uso de contraseñas y acceso a los equipos e información crítica y confidencial.
- La protección de las instalaciones. En el Grupo VILOR, todos los entornos de desarrollo y almacenamiento de información crítica están ubicados en un HOSTING externo y seguro, debiendo protegerse de manera local los elementos periféricos y portátiles, que componen en sistema de seguridad de la información.

No obstante, si fuera necesario, está prevista la protección de las instalaciones, infraestructuras de almacenamiento de la información crítica y confidencial y restantes recursos físicos relacionados con el sistema de seguridad de la información, mediante el establecimiento de límites físicos, de control de accesos, de cuidado de las instalaciones ante factores ambientales y emergencias, incluyendo posibles planes de contención, de actuación, de vigilancia, etc.

- El diseño y configuración del sistema de seguridad de la información con mínimos privilegios, adaptado a las necesidades, objetivos y requisitos del Grupo VILOR y sus clientes, garantizando su correcto funcionamiento y desempeño.
- La adquisición de productos, gestión de cambios y contratación de servicios, relacionados con nuestro sistema de seguridad de la información, centralizados y supervisados por el departamento TIC, desde su adquisición hasta su retirada, para garantizar que disponen de los certificados y garantías mínimas requeridas durante todo su ciclo de vida, estableciéndose un proceso de seguridad integral y transversal, con adopción de medidas compensatorias si fuera necesario, para cumplir, mantener y garantizar el nivel de seguridad ALTO.
- La integridad y actualización del sistema, a través del proceso de control de la gestión de los cambios y actualizaciones de los elementos físicos y/o lógicos, con evaluación y autorización previa a su instalación, por el departamento TIC, documentando y planificando los cambios significativos para el sistema de seguridad de la información, así como controlando su evolución y desarrollo.
- La protección de la seguridad almacenada y en tránsito, implantando medidas de protección en los entornos inseguros, para nuestro sistema de seguridad de la información: equipos portátiles, dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas, con cifrado débil, etc.
- La prevención ante otros sistemas de información interconectados, implantando medidas de protección del perímetro crítico, previas a la interconexión, y analizando los riesgos de las interconexiones y controlando su punto de unión, a posteriori, especialmente, ante la conexión a redes públicas y/o para prestar servicios de comunicaciones electrónicas disponibles para el público.
- El registro de actividad y códigos dañinos, implantando registro de control de actividad de los usuarios, permitiendo identificar en cada momento de manera inequívoca a la persona que actúa, promoviendo la eficiencia empresarial y reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, así para clasificar la actuación en el registro de incidencias, y activar la alarma y plan de contención, de manera urgente.
- La detección de incidentes y continuidad de la actividad, a través del seguimiento continuo y monitoreo de los procesos, para detectar de manera anticipada dichas amenazas y riesgos, en el tratamiento de datos personales e información crítica y confidencial, la gestión y tratamiento de los incidentes, amenazas y riesgos, etc., y para realizar las copias de seguridad y adoptar las medidas que sean necesarias para mantener la protección de la información crítica y garantizar la prestación continua del servicio.
- La mejora continua del sistema de seguridad de la información, a través de la valoración de los resultados de medición de los indicadores de los procesos de seguridad de la información, del funcionamiento de las medidas preventivas aplicadas, del análisis de los incidentes de seguridad y las medidas correctivas implantadas para solucionarlos, etc., y conforme a los estándares de seguridad, criterios y metodologías establecidas en el Esquema Nacional de Seguridad.

Esta Política está diseñada para toda la plantilla del Grupo VILOR y recursos externos que presten sus servicios a las empresas del Grupo VILOR, quienes deben cumplir y hacer cumplir estas directrices para proteger la seguridad de la información que se maneje por parte de cualquier recurso del Grupo VILOR.

Valencia, a 19 de diciembre de 2025
La Dirección (Grupo VILOR)