Política de Seguridad de la Información

DGH robótica, automatización y mantenimiento industrial, S.A.

1 Política Seguridad Información

La **Política de Seguridad de la Información** de DGH parte del compromiso, por parte de la Alta Dirección, de garantizar la plena satisfacción de los grupos de interés de la organización, así como la gestión de la seguridad de sus sistemas de información.

DGH enfoca la Seguridad de la Información como un sistema de gestión para entregar productos o prestar servicios que satisfagan las necesidades del cliente; teniendo en cuenta los requisitos de la actividad de la organización, así como los requisitos legales, reglamentarios o contractuales. Todos los procesos internos y externos quedan adscritos y afectados a la presente política, o a cuantas otras políticas transversales se desarrollen para dar cumplimiento a la misma.

La Política de SI tiene vigencia desde la aprobación por la Dirección y se mantendrá vigente mientras no se apruebe una posterior. La Política es comunicada y puesta a disposición de todos los afectados, tanto internos como externos.

Toda violación de la presente política o de aquellas que la desarrollen, de las normas y procedimientos correspondientes, será evaluada, tratada y, en su caso, sancionada de acuerdo con los procedimientos previstos al efecto, incluidos proveedores y colaboradores externos.

2 Compromisos de la Dirección.

La Alta Dirección de DGH está comprometida con el desarrollo e implementación del Sistema de Seguridad de la Información, y con la mejora continua de su eficacia.

La Directora de Organización y Calidad de DGH dirige el Sistema Integrado de Gestión (SIG), y por tanto también es la Directora del Sistema de Gestión de Seguridad de la Información; el resto de los miembros del equipo directivo de la organización están, asimismo, comprometidos con la seguridad de la compañía, además de por sus cargos, por formar parte del Comité de Seguridad de la Información.

La Directora de Organización y Calidad:

- Comunica a la organización la importancia de satisfacer tanto los requisitos del cliente como los de seguridad, los legales, reglamentarios, y las obligaciones contractuales.
- Establece y comunica el alcance del SSI.
- Define y comunica la Política del Sistema Seguridad de la Información, normas y procedimientos.
- Comunica la Política de Seguridad y la importancia de cumplir con ella a clientes y a proveedores (contrato de confidencialidad).
- Asegura el establecimiento y la comunicación de los objetivos de calidad y de seguridad de la Información.
- Lleva a cabo las revisiones por la Dirección anuales.
- Dirige las revisiones del Sistema de Gestión.

- Vela por que se realicen las auditorías internas del SSI, anualmente.
- Asegura que se revisan los resultados de las auditorías para identificar oportunidades de mejora.
- Asegura la provisión y disponibilidad de recursos.
- Asegura que se gestionan y se evalúan los riesgos de seguridad de la información, a intervalos planificados.
- Define el enfoque a tomar para la gestión de los riesgos de seguridad de la información y los criterios para asumir los riesgos.
- Aprueba los niveles de riesgo aceptables para la organización.
- Establece roles y responsabilidades en materia de seguridad.
- Determina las cuestiones externas e internas que son pertinentes para el propósito de la organización y su dirección estratégica.

El compromiso de la Dirección está reflejado en las siguientes políticas.

3 Objetivos Política de Seguridad de la Información

La Política de Seguridad tiene por objeto proteger los activos de información del sistema de información de DGH, así como los activos de información de nuestros clientes con los que exista un acuerdo contractual, ante cualquier amenaza, sea interna o externa, deliberada o accidental. Se busca garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con urgencia a los incidentes para recuperarse lo antes posible y minimizar el impacto.

DGH tiene implantado, y mejora continuamente, un Sistema Gestión de la Información acorde con las normas UNE-**ISO/IEC 27001:2013** y **TISAX** (Trusted Information Security Assessment Exchange) es un estándar de seguridad impulsado por la VDA, que recoge los requisitos fundamentales de la norma ISO 27001 seguridad de la información y los adapta a la industria automotriz.

La Política de Seguridad de la Información se aplica a todas las personas de la organización, incluyendo sus contratistas y el personal contratado temporalmente; afecta a cualquier tipo de información, tanto la que sea propiedad de la organización como la que procede de clientes, con independencia del soporte o medio en el que se encuentre, tipología o categoría; y aplica a cualquier activo de información propiedad de la organización que afecte al sistema.

La Seguridad de la Información está implícita en cada uno de los puntos de esta Política, e integrada en los procesos de negocio como herramienta clave para conseguir los objetivos de negocio de la organización. Esta política queda alineada plenamente con los objetivos de negocio e integrada en la estrategia de la organización.

3.1 Objetivos

Los objetivos del Sistema de Gestión relacionado con Seguridad de la Información de la organización son:

- Mantener una gestión adecuada del Sistema de Gestión de acuerdo con los estándares de seguridad y las buenas prácticas del sector, llevando a cabo todo esto de manera que se aseguren ventajas competitivas para la organización.
- Proteger la información interna relacionada con la prestación de los servicios, considerando las dimensiones de:
    - Confidencialidad para asegurar que la información sólo sea accesible a aquellas personas que cuenten con la autorización respectiva. Toda la información se protegerá, de manera que no se pondrá a disposición, ni se revelará, a individuos, entidades o procesos no autorizados previamente.
    - Integridad para preservar la veracidad y completitud de la información y los métodos de procesamiento. Toda la información se protegerá de manera que se podrá asegurar que no ha sido alterada de manera no autorizada. La alteración será entendida en todos sus contextos, es decir, la creación, modificación o eliminación.
    - Disponibilidad para asegurar que los usuarios autorizados tienen acceso a la información y los procesos, sistemas y redes que la soportan, cuando se requiera. Será principio básico de DGH, la restricción de accesos al mínimo nivel necesario.
- Establecer anualmente objetivos específicos en relación con la Seguridad de la Información, que garanticen la mejora continua del Sistema de Gestión, siendo estos consistentes con los actuales objetivos.
- Desarrollar un proceso de análisis del riesgo y, de acuerdo con su resultado, implementar las acciones correspondientes con el fin de tratar los riesgos que se consideren inaceptables, según los criterios establecidos en IT08 P01 Análisis Riesgos.27001.
- Establecer los medios necesarios para garantizar la continuidad del negocio de la organización.
- Cumplir con los requisitos del negocio, las obligaciones legales y las obligaciones contractuales de seguridad.
- Asegurar que los activos de la organización solo sean utilizados por usuarios autorizados en el ejercicio de sus funciones, sus perfiles definidos o según asignaciones extraordinarias.
- Establecer y difundir los roles y responsabilidades relacionados con la Seguridad de la Información que están identificados en la Descripción de Puesto de Trabajo.
- Sensibilizar y concienciar de manera estable y permanente a todo el personal de DGH en cuanto a la seguridad de la información.
- Fomentar y mantener el buen nombre de DGH en relación con los servicios desarrollados, y dar una respuesta activa (reactiva y proactiva) ante incidentes de seguridad, manteniendo y mejorando la imagen y reputación.
- Reflejar en la Declaración de Aplicabilidad los objetivos de control definidos, basados en los controles recogidos en el Anexo A de la norma 27001:2013.
- Sancionar cualquier violación a esta política, así como a cualquier política o procedimiento del Sistema de Gestión.