

## POLÍTICA INTEGRADA DE GESTIÓN DEL SERVICIO, SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS

La **Dirección de Diusframi** quiere dar a conocer, a través de este documento, a sus trabajadores, clientes, proveedores y otras partes interesadas su convencimiento de que la Gestión de Servicios de TI, la Seguridad de la Información y la Protección de Datos, son un factor clave para el correcto desarrollo de la organización y se establece como objetivo fundamental la mejora continua de nuestros servicios de:

- “Mantenimiento correctivo y evolutivo, de instalación, integración, operación, explotación y soporte técnico de sistemas de información propios y de clientes (aplicaciones, redes e infraestructuras TIC), de acuerdo con el catálogo de servicios vigente.”
- “Los sistemas de información necesarios para las actividades de los servicios de diseño, desarrollo, instalación, integración, operación, explotación, soporte técnico y mantenimiento de sistemas de información (aplicaciones, redes e infraestructuras TIC) propios y de clientes, según la declaración de aplicabilidad vigente a fecha de emisión del certificado.”

Con el fin de garantizar la calidad y excelencia en la gestión del servicio de TI y del tratamiento de la información, se ha desarrollado e implantado un Sistema integrado de Gestión del Servicio de TI y de la Seguridad de la Información, con el compromiso de cumplir con los requisitos exigidos por las normas UNE-ISO/IEC 20000-1 y UNE-ISO/IEC 27001.

Esta política se establece como marco en el que se deben desarrollar todas las actividades de **Diusframi**, de manera que se garantice a los clientes y demás partes interesadas el compromiso adquirido, para asegurar la disponibilidad, la confidencialidad y la integridad de la información, así como el establecimiento de los objetivos de Gestión de Servicios de TI y la Seguridad de la Información.

Para todo ello, la **Dirección de Diusframi**, define esta política, quedando a disposición para todos nuestros clientes y partes interesadas pertinentes y que es el marco de referencia para el establecimiento de los objetivos de Gestión de Servicios de TI, la Seguridad de la Información y Protección de Datos, y adquiere los siguientes compromisos:

- Mantener el conjunto de capacidades y procesos que permitan dirigir y controlar las actividades y recursos de la organización para la planificación, diseño, transición, entrega y mejora de los servicios con la finalidad de entregar valor al cliente, cumpliendo con sus requisitos tanto de nivel de servicio como de seguridad de la información.
- Asegurar que los servicios prestados se hallan alineados con las necesidades de sus clientes y usuarios.
- Implantar y mantener un sistema de mejora continua del Sistema de Gestión del Servicio de TI y de la Seguridad de la Información
- Mantener la comunicación entre el personal que participa en la prestación de los servicios, y los clientes y usuarios de dichos servicios.
- Incrementar la eficacia y eficiencia de los procesos internos del Sistema de Gestión del Servicio de TI y de la Seguridad de la Información.
- Crear un entorno de trabajo que fomente la participación de nuestros trabajadores de cara a lograr la satisfacción de nuestros clientes.
- Garantizar la protección de datos personales y el cumplimiento de todas las obligaciones exigibles en esta materia.

En resumen, mantener un servicio de calidad a nuestros clientes y usuarios, a través del uso de procesos de trabajo en revisión constante, con un equipo humano altamente capacitado y comprometido en todos sus niveles para alcanzar la excelencia en los servicios prestados.

Para garantizar el cumplimiento de estos compromisos, se realizan las siguientes acciones:

- Nombrar un responsable que se encargue de gestionar el sistema y vele por el desarrollo, mantenimiento y mejora de este.
- Nombrar un Delegado de Protección de Datos personales que vele por el cumplimiento de la normativa vigente en esta materia.
- Efectuar un análisis de las necesidades existentes en torno a la prestación de servicios y desarrollar las actividades necesarias para ofrecer una respuesta adecuada a dichas necesidades.
- Cumplir todos los requisitos aplicables a la seguridad de la información y protección de datos, (legales, normativos y reglamentarios), los requisitos del cliente y cualquier otro requisito asumido por la Dirección de Diusframi.
- Desarrollar una completa estructura de gestión que regule las condiciones en las que la organización, debe desarrollar su actividad.
- Destinar los recursos y medios necesarios para gestionar los servicios TI y la seguridad de la información y protección de datos exigidos, manteniendo un adecuado balance entre coste y beneficio.
- Establecer un plan de formación y concienciación tanto en materia de gestión de servicios, que ayude a conocer y cumplir las actividades de gestión, como en materia de seguridad de la información y protección de datos, que garantice el conocimiento por parte del personal de Diusframi, de las políticas, los procedimientos, los controles y medidas de seguridad y privacidad aplicadas y que fomente la participación activa en el desempeño de la seguridad de la información, protección de datos y gestión de los servicios.
- Asegurar la protección de los activos de la organización y monitorizar el desempeño de proveedores.
- Establecer los mecanismos apropiados que permitan la gestión de incidentes que pudieran interrumpir o comprometer las operaciones de negocio, diseñando e implantando mecanismos que permitan su prevención, detección, control, recuperación y posterior análisis.
- Establecer periódicamente un conjunto de objetivos e indicadores, que permitan a la dirección llevar a cabo un adecuado seguimiento de los niveles de servicio ofrecidos y las actividades de gestión, así como el desempeño de la seguridad de la información y protección de datos.
- Establecer una metodología de revisión, auditoría y mejora continua del sistema siguiendo un ciclo PDCA que garantice el mantenimiento continuo de los niveles de calidad deseados, así como el aseguramiento del cumplimiento con las leyes y regulaciones aplicables, y otras obligaciones a las cuales se suscriba a fin de satisfacer las expectativas de las partes interesadas pertinentes.
- Establecer un proceso de medición de la satisfacción del cliente con respecto a los servicios prestados, permitiendo identificar y priorizar acciones de mejora que permitan incrementar el nivel de satisfacción.
- Hacer uso del “Sistema de Gestión de Seguridad de la Información” como una herramienta para implementar un sistema formal, y que define las directrices generales relacionadas con la Seguridad de la Información a fin de Asegurar la Seguridad de la información en los proyectos y servicios prestados, protegiendo sus activos de información al nivel requerido de Disponibilidad, Confidencialidad e Integridad, mediante la aplicación y seguimiento de las políticas, normas y procedimientos relativos a la gestión del servicio de TI y seguridad de la información.

- Actuar ante anomalías e incidencias que puedan surgir, en su comunicación, documentación y resolución.
- Implementar planes de continuidad y disponibilidad del negocio, que garanticen la prestación de los servicios, manteniendo los niveles de gestión y seguridad necesarios.
- Realizar evaluaciones de riesgo periódicas (o con cada cambio crítico) del estado de la seguridad de la información y protección de datos, que identifique amenazas y vulnerabilidades, y cuyo tratamiento proporcione mecanismos para mitigar los riesgos asociados al cumplimiento de los requisitos operativos.
- Asegurar que de los datos de tarjetas se tratan como información confidencial, y, por lo tanto, las medidas de seguridad a aplicar en ellos serán las relativas a información de dicho nivel.
- Velar por que las instalaciones de la compañía cuenten con las medidas de seguridad física necesarias para garantizar un nivel adecuado de protección, frente a potenciales amenazas.

Todo ello manteniendo el compromiso de Diusframi en minimizar su impacto ambiental y social, y en la transición hacia un futuro sostenible, mientras promueve el bienestar de sus empleados y las comunidades en las que opera, incorporando progresivamente las oportunidades y riesgos relativos al cambio climático y desarrollo social inclusivo en su estrategia, procesos y gestión de riesgos.

En este sentido, el código de conducta de Grupo Diusframi sirve como declaración y compromiso en la implantación y desarrollo de unos principios éticos basados en la integridad y la transparencia en la transición hacia un futuro sostenible, inspirándose en los Objetivos de Desarrollo Sostenible (los “ODS”) adoptados por la Organización de las Naciones Unidas, y en otros organismos supranacionales.

La presente política es conocida y suscrita por todo el personal de Diusframi conforme a las exigencias de la dirección, y será revisada con una periodicidad máxima anual, siendo sus cambios debidamente aprobados por la dirección de la organización, como es el caso en Madrid a 20 de diciembre de 2024.

José Luis Delgado  
Dirección General

(La presente política es firmada por la Dirección de TI actuando en representación de la Dirección General.)

Ignacio Rodríguez  
Dirección TI

GRUPO DIUSFRAMI  
Diciembre 2024

La presente política ha sido redactada utilizando el lenguaje masculino como género indiferenciado, con el propósito de incluir tanto a hombres como a mujeres, en línea con nuestro compromiso de promover una política inclusiva que respete la igualdad de género en todas nuestras prácticas y comunicaciones.