Código: SGI-P-01 **Edición:** 02	**SISTEMA DE GESTIÓN INTEGRAL DESTRUCCIÓN CONFIDENCIAL DE DOCUMENTACIÓN S.A.**		
	TITULO: *"Política general del Sistema de Gestión Integrado"*		
	Fecha elaboración: 01/2015	Fecha revisión:	24/05/2024
Elaborado por: Rble. Normativo y certificaciones		Michael Javier Ramirez	
Revisado por: C.S.I.		Cristina Rodrigo Aguilera	
Aprobado por: Directora general		Cristina Rodrigo Aguilera	

DCD, S.A es **líder en el Outsourcing de Destrucción Confidencial de Documentación** en España desde 1996. Sin inversiones iniciales para el cliente ni costes fijos, gestiona más de 9.500 puntos de recogida, trabaja en más de 2.500 edificios y ha conseguido obtener la confianza, de más de usuarios, llegando a destruir confidencialmente más de 8 millones de kilos por ejercicio.

La dirección de DCD tiene atribuidas las competencias de diseñar, evaluar y revisar los Sistemas de gestión y por tanto de aprobar las políticas corporativas en las que se recogen las líneas de actuación de la Sociedad.

Nuestra misión, visión y valores son los pilares fundamentales que nos han llevado a conseguirlo, que conforman nuestra identidad, nos dan coherencia y diferencian de nuestra competencia.

Nuestra misión:

Destruir la información sensible o protegida por LOPD de las empresas u organismos en cualquier tipo de soporte, mediante un proceso confidencial y con alta capacidad de destrucción industrial, cumpliendo los más altos estándares de calidad y seguridad siendo respetuosos con el medio ambiente y aportando valor en nuestro entorno social.

Nuestra visión:

La búsqueda del cumplimiento de nuestros compromisos, avance tecnológico y la voluntad de unos servicios completamente confidenciales para liderar el mercado siendo la empresa de referencia.

Nuestros valores:

- **Responsabilidad**: con el cumplimiento y con el entorno del que formamos parte.
- **Medio ambiente:** la preservación del medio ambiente y el fomento de actuaciones consecuentes con nuestra razón de ser.
- **Honestidad e integridad:** con nuestros clientes, empleados y con todos aquellos que colaboran en el desarrollo de nuestra actividad.
- Generar **confianza** gracias a nuestra pasión por el trabajo bien hecho y la voluntad de seguir liderando nuestro mercado.
- **Compromiso** con nuestros principios éticos y la transparencia.

Consciente del compromiso que representan y teniendo en cuenta a todas las partes implicadas, empresas colaboradoras, autoridades, trabajadores y la sociedad en general, la Dirección de DCD para el cumplimiento de los dispuesto en esta visión y estos valores ha aprobado las siguientes Políticas de Calidad y Medio Ambiente, Seguridad y Privacidad de la Información y de los datos y todos aquellos elementos estratégicos de la compañía que son de aplicación a todos los servicios a prestar, a todas sus instalaciones y a todos su empleados.

POLITICA DE CALIDAD Y MEDIOAMBIENTE

La política de Calidad y Medio Ambiente de DCD se sustenta en las siguientes premisas:

- Un enfoque de mejora continua en búsqueda de la excelencia en todas las actuaciones de la empresa con el objetivo de conseguir la satisfacción del cliente mediante la calidad en la prestación del servicio y la optimización en la utilización de Recursos.
- Desarrollar la actividad de la empresa cumpliendo con la reglamentación vigente y los requisitos contractuales, así como cualquier requisito que nuestra organización suscriba voluntariamente.
- Mediante procesos de control y de mejora continua establecer medidas y acciones orientadas a la detección, superación y prevención de problemas.
- Administrar los Recursos materiales proporcionando los medios necesarios para la conservación y modernización de equipos e instalaciones optando por soluciones que reduzcan las emisiones y la generación de energías renovables.
- Hacer uso responsable de los recursos materiales y energéticos y minimizar la generación de residuos.
- Gestionar el equipo humano conscientes del enorme valor que aportan a la Organización a través de la formación y desarrollo continuo de todos los trabajadores de la compañía.
- Asegurar la disponibilidad de información, la difusión de los compromisos y los recursos necesarios para alcanzar los objetivos y las metas del Sistema integrado.
- Evaluar y revisar de forma periódica los Sistemas de Gestión para reflejar los cambios en las condiciones, en la información y evaluar los objetivos trazados.
- Estas premisas proporcionan el marco de referencia por el cual se establecerán objetivos en relación con los siguientes aspectos:
- Garantizar el cumplimiento de la legislación, los requisitos contractuales y demás normativa vigente aplicable.
- Fomentar la excelencia mediante la aplicación de la tecnología, ambiente de trabajo e infraestructura adecuada y el desarrollo del talento humano.
- Gestionar la empresa respetando los principios de integridad, calidad de servicio, liderazgo y equipo comprometido.
- Promover la satisfacción del cliente mediante el cumplimiento de sus expectativas y la mejora continua de los servicios prestados.
- Promover el ahorro energético y la utilización racional de los recursos naturales.
- Optimizar la gestión de residuos.

POLITICA DE SEGURIDAD Y SALUD EN EL TRABAJO

La Política de DCD establece el compromiso de proporcionar condiciones de trabajo seguras y saludables y aportar a los trabajadores una protección eficaz frente a los riesgos laborales, con el fin de elevar los niveles de seguridad, salud y bienestar de la propia organización mediante la integración de esta cultura en la gestión global de la Organización, de tal forma que todas las actividades son consideradas desde una perspectiva de prevención de todo tipo de accidentes y protección de las personas en el entorno laboral.

Por estas razones, **DCD** adquiere los compromisos que siguen a continuación:

- Dotar de los recursos humanos, económicos y materiales necesarios para alcanzar los objetivos en materia de prevención de riesgos.
- Desarrollar todas las actividades preventivas específicas de las especialidades de seguridad en el trabajo, higiene industrial, ergonomía y psicosociología aplicada, junto con el área de vigilancia de la salud en la especialidad de medicina del trabajo.
- Alcanzar un alto nivel de seguridad y salud en el trabajo, cumpliendo con los requisitos legales y otras obligaciones vigentes en materia de Prevención de Riesgos Laborales, así como con otros requisitos adicionales asumidos como propios.
- Definir estrategias que fomenten la cultura de prevención, bienestar y salud en todos los niveles de la organización.
- Garantizar la protección contra incendios mediante la introducción de normas y medidas mínimas para mitigar los riesgos y asegurar la continua mejora de la seguridad contra incendios proporcionando a todo el personal el entrenamiento correspondiente.
- Asegurar las protecciones en los centros de trabajo, en la maquinaria y vehículos, así como una eficaz adecuación de los lugares de trabajo garantizando los mantenimientos preventivos y correctivos correspondientes.
- Implementar, probar y evaluar, así como formar a los trabajadores, en los procedimientos y actividades para hacer frente a una situación de emergencia o desastres asegurando una respuesta apropiada ante estas situaciones.
- Desarrollar actividades formativas e informativas en prevención de riesgos laborales con el fin de procurar comportamientos seguros en todo el equipo humano estableciendo los cauces necesarios para garantizar el reciclaje formativo.
- Proporcionar y asegurar el uso de los equipos de protección individual (EPI's) necesarios en cada puesto de trabajo y actividad.
- Establecer los métodos apropiados para el registro e investigación de accidentes e incidentes que se produzcan, así como la aplicación correcta de las medidas preventivas derivadas de la investigación de estos y la adecuación de los documentos relativos a la Prevención de Riesgos Laborales.
- Fomentar la participación de los empleados en las cuestiones relacionadas con la promoción de la salud y bienestar.
- Impulsar en nuestra cadena de suministro y con nuestros socios las mejores prácticas en materia de seguridad, salud y bienestar.
- Establecer objetivos y metas de mejora, teniendo en cuenta los requerimientos de nuestros grupos de interés de forma sistemática, evaluar el desempeño de forma continua, aplicando las correcciones necesarias para alcanzar los logros propuestos.

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

DCD vela por la protección de la información, independientemente de la forma en la que esta se comunique, comparta, proyecte o almacene para lo cual la Dirección de **DCD** ha establecido esta Política de Seguridad y Privacidad de la información.

Esta política constituye el marco de referencia mediante el que se definen las directrices de protección eficaz de la información y de los datos de carácter personal de cualquiera de las partes interesadas (empleados, clientes, proveedores, Administración Pública, otros terceros ...) en cualquier soporte y en todos los procesos y tratamientos que se llevan a cabo mediante la generación y publicación de normativas, procedimientos e instrucciones técnicas así como de la asignación de responsabilidades generales y específicas.

En base a estándares internacionales de seguridad de la información y aplicando el principio de protección de datos desde el diseño y por defecto se sientan las bases para que el acceso, uso, custodia y salvaguarda de los activos de información, se realicen bajo garantías de seguridad en sus distintas dimensiones (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) así como para asegurar que la organización está preparada para prevenir, detectar, reaccionar y recuperarse de incidencias.

Se encuentran definidos los roles de Seguridad, incluido el responsable de Seguridad, junto con sus funciones y responsabilidades, así como los mecanismos de renovación de estos roles.

En función de lo expuesto anteriormente la Dirección de **DCD** asume y dispone los compromisos con respecto a la seguridad y privacidad de la información:

- El cumplimiento de la normativa de seguridad y privacidad respetando de forma escrupulosa la legalidad vigente.

Marco normativo:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPD).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS)
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- UNE - ISO/IEC 27001:2013 Sistema de Gestión de la Seguridad de la información.
- UNE-EN ISO 9001:2015 Sistema de Gestión de la Calidad
- UNE-EN ISO 14001:2015 Sistema de Gestión Ambiental
- UNE-EN 15713:2010 Sistema de Gestión de la Destrucción Segura de Material Confidencial (Buenas prácticas)

Nota: A demás aquellas aplicables en el Normograma corporativo

- La integración de la seguridad y la privacidad en los procesos de negocio, como un componente más de los mismos.
- Llevar a cabo el tratamiento de datos personales a partir de los principios de licitud, transparencia, minimización de datos, exactitud, retención y eliminación y confidencialidad y seguridad recogidos en el RGPD.
- La adopción de un modelo de seguridad que cubra la protección de los activos y procesos de negocio en cada etapa de su ciclo de vida frente a los riesgos de seguridad y privacidad de cualquier naturaleza, prestando especial atención a los Ciber riesgos.
- Poner los medios organizativos y técnicos necesarios para evaluar regularmente la seguridad y garantizar la mejora continua del sistema cumpliendo con el principio de "Accountability".
- Garantizar a los interesados el ejercicio de sus derechos de acceso, rectificación, oposición, supresión, limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas.
- Implementar, mantener y realizar un seguimiento de los controles contenidos en su declaración de aplicabilidad y los procesos del SGSI, conforme a las normas ENS e ISO 27001 principalmente.
- Formar, concienciar a todo el personal y proveedores en materia de seguridad y privacidad, así como la divulgación de normas, procedimientos y responsabilidades.
- Cumplir su obligación de secreto con respecto a los datos de carácter personal y al deber de tratarlos con confidencialidad. A estos efectos, adoptará las medidas necesarias para evitar su alteración, pérdida, tratamiento o acceso no autorizado.
- Compromiso de la organización con la mejora continua con el sistema de gestión de seguridad de la información.
- Identificar a los responsables de la información, que deberán promover el establecimiento de los controles y medidas destinadas a proteger los datos, la información, los activos, la continuidad del servicio y los sistemas de información mediante la asignación de roles, responsabilidades y autoridades.

Comité de seguridad: Funciones y responsabilidades

Responsable de Seguridad	Michael Javier Ramirez Ávila
Responsable de la Información	Cristina Rodrigo Aguilera
Responsable del Servicio	Cristina Rodrigo Aguilera
Responsable de Sistemas	Ricardo Bardina Pastor

Responsable de seguridad

- Convoca reuniones del CSI
- Genera las actas de reunión del CSI.
- Genera los planes de tratamiento de gestión de riesgo y supervisa su implantación.
- Gestiona los incidentes de seguridad y las acciones correctivas correspondientes.
- Actualiza el análisis de riesgos.
- Supervisa la recogida de métricas.
- Mantiene los documentos del SGSI.
- Mantiene y despliega la política de seguridad de DCD.
- Ejecuta la auditoría de seguridad de protección de datos.
- Realiza las revisiones de seguridad del SGSI.

- Mantiene el Plan de Continuidad de Negocio.
- Departamento de LOPD.
- Elabora, o participa en la elaboración, de los documentos de seguridad de DCD, en su caso.
- Elabora los acuerdos para el tratamiento de datos por terceros.
- Atiende consultas en materia de protección de datos.

Responsable de Sistemas

- Supervisa, otorga, modifica los perfiles de acceso de usuarios
- Controla el acceso de personas a los locales donde están instalados los sistemas.
- Lleva el inventario de soportes que contienen datos de carácter personal.
- Supervisa el registro de entrada y salida de soportes que contienen datos de carácter personal.
- Supervisa el registro de incidencias en los ficheros a los que se aplica el nivel alto de seguridad.
- Analiza los informes de auditoría y elevan las conclusiones al responsable del fichero.
- Supervisa las incidencias de seguridad producidas.
- Administra los sistemas de la red
- Lleva el inventario de sistemas, programas y hardware.
- Implanta y gestiona la seguridad de sistemas, red, servicios, etc.
- Mantiene las copias de seguridad.
- Lleva el registro de entrada y salida de soportes.
- Atienden las incidencias de tipo técnico que afectan a los sistemas.
- Elabora, o participa en la elaboración, de los documentos de seguridad de DCD, en su caso.
- Mantienen los servidores y los ordenadores de los departamentos o áreas de DCD.
- Instala las aplicaciones en fase de producción.
- Define los perfiles de acceso de usuarios.
- Dan de alta o baja a los usuarios.
- Genera la relación de usuarios con acceso al sistema/aplicaciones especificando los niveles de acceso.

Responsable del Servicio - Información

- Promueve y dirige la política de seguridad de la información.
- Aporta los recursos financieros para la misma.
- Aprueba el sistema de gestión de seguridad de la información.
- Aprueba la política de seguridad de la información.
- Aprueba los riesgos de seguridad.
- Designa a los responsables de seguridad de ficheros.
- Aprueba el Plan de Continuidad de Negocio

Comité de Seguridad de la Información

- El CSI analiza el estado de la política de seguridad de DCD.
- Participa en la confección de directrices generales.
- Contribuye a la revisión de la política de seguridad de la información.
- Designa, revisa y renueva los roles de seguridad de la información y sus funciones,
- bien cuando existan cambios significativos en el personal o cada tres años.
- Realiza reuniones periódicas.
- Adopta las medidas necesarias para que el personal interno conozca y se responsabilice en el cumplimiento de las normas de seguridad o de protección que

afecten al desarrollo de sus funciones.

- Revisa toda la documentación relacionada con el SGSI.
- Impulsa la elaboración procedimientos técnicos, jurídicos y organizativos que sean necesarios para el cumplimiento de la normativa.
- Sensibiliza al personal, mediante campañas o sesiones formativas o de sensibilización
- Resuelve, en última instancia, el ejercicio de los derechos de los afectados.
- Detecta las necesidades en materia de seguridad e impulsa las soluciones para cubrirlas.
- Controla el cumplimiento de la normativa por las empresas externas que realizan tratamientos para DCD.
- Apoya de modo claro la revisión y mantenimiento y la mejora continua del SGSI demostrando así el apoyo y compromiso de la Dirección de DCD para con dicho sistema.
- Revisa la adecuación y efectividad del SGSI, evaluando las oportunidades de mejora.
- Define el nivel de riesgo asumible.
- Aporta recursos para la mejora del SGSI.

➢ Bajo estos compromisos se desarrollan los objetivos de la Seguridad y Privacidad de la información que garantizan:

Objetivos:

- ❖ El gobierno de la seguridad de la información, sobre la base de procesos de análisis de riesgos.
- ❖ La gestión de la reacción y la recuperación ante cualquier incidente, desarrollando planes de continuidad conformes a metodologías de reconocido prestigio internacional.
- ❖ Establecer las medidas técnicas y organizativas adecuadas para salvaguardar la confidencialidad y seguridad de la información y de los datos de carácter personal que tratamos.
- ❖ Una adecuada gestión de incidencias que afecten a la seguridad de la información y a las brechas de seguridad de los datos incluyendo la mitigación, remediación y recuperación.
- ❖ La satisfacción de las expectativas y necesidades en materia de seguridad de clientes, empleados, proveedores, Dirección, Socios, Autoridades/Reguladores, usuarios y demás partes interesadas.
- ❖ La protección de los derechos de propiedad intelectual e industrial.
- ❖ La correcta verificación del cumplimiento de las medidas, normas y procedimientos establecidos en esta Política, de tal forma que pueda detectarse cualquier anomalía que afecte a la seguridad, integridad o disponibilidad de los datos personales contenidos en los ficheros, se realizarán, controles periódicos

Para notificar su cumplimiento se firma en San Martín de la Vega, a 24 (veinticuatro) de mayo de dos mil veinticuatro.

Dirección General

CRISTINA RODRIGO AGUILERA