DesideDatum

We build data-driven organizations

25 de julio de 2024

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Ficha del documento

Información del documento		
Autor del documento:	**Manuel Rato**	Versión: 1.0
Fecha creación	**024/07/2024**	Baja documento:

Historial de versiones					
Versión	**Cambios**	**Tipo**	**Responsable**	**Nombre**	**Fecha**
1.0	CSI	Redacción	Seguridad-IT	Manuel	24/07/2024
1.0	CSI	Revisión	Comité de la Seguridad de la Información	N/A	25/07/2024
1.0		Aprobación	Dirección	Marc Garriga	25/07/2024

ÍNDICE

2. Objetivo y descripción del documento

Declaración de Propósito:

La información y los servicios proporcionados por **Desidedatum Data Company** representan activos fundamentales para la organización y, como tal, requieren una protección integral contra amenazas y riesgos. La Dirección de **Desidedatum Data Company** apoyará y aprueba formalmente la presente Política de Seguridad de la Información (PSI) con el fin de establecer una estrategia coherente para salvaguardar la integridad, confidencialidad y disponibilidad de la información, así como para asegurar la continuidad de los servicios.

Objetivos estratégicos:

Contribución a los Objetivos Institucionales: La gestión de la seguridad de la información se concibe como un elemento estratégico alineado con los objetivos de **Desidedatum Data Company**, contribuyendo activamente a su cumplimiento.

Cumplimiento Legal y Regulatorio: Se implementarán medidas de control para garantizar el cumplimiento de los requisitos legales y regulatorios, con un enfoque especial en la protección de datos personales y servicios electrónicos.

Integridad, Confidencialidad y Disponibilidad: La política se orienta a asegurar la integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad de la información, así como a mantener la prestación ininterrumpida de los servicios.

Protección de Recursos de Información y Tecnología: Se establecerán y mantendrán medidas de protección para salvaguardar los recursos de información y la tecnología utilizada, mitigando amenazas internas y externas.

Compromiso con la Mejora Continua:

Desidedatum Data Company manifiesta su compromiso con la mejora continua en la gestión de la seguridad de la información. Este compromiso es liderado por el Departamento de Seguridad de la Información, cuyas responsabilidades abarcan integralmente todas las áreas de la organización. Se asignarán los recursos necesarios para garantizar una gestión efectiva y evolutiva de la seguridad de la información en consonancia con las mejores prácticas y estándares del sector.

3. Ámbito de aplicación

La presente política afecta a los sistemas de información y a la información misma gestionados o supervisados por **Desidedatum Data Company**. Es de aplicación y obligado cumplimiento para todas las unidades, áreas, subáreas y servicios de **Desidedatum Data Company**, así como para cada una de las sociedades que integran **Desidedatum Data Company**, sobre las que se ejerce un control efectivo, es decir, todo aquello que forme parte de la organización.

Además, **Desidedatum Data Company** velará que los principios establecidos en la Política de Seguridad de la Información (PSI) se adviertan a terceros que presten servicios o colaboren con la compañía, como clientes, asesores, agentes, proveedores, etc.

Concienciación y Participación Activa:

Es esencial que los profesionales de **Desidedatum Data Company** sean plenamente conscientes de la importancia de la seguridad de la información en su actividad diaria. Así pues, fomentaremos la participación activa de todos en el desarrollo y la mejora continua de la seguridad de la información, contribuyendo así a la creación de un entorno más seguro para todos.

4. Principios rectores

Principios Básicos de la Política de Seguridad de la Información:

La Política de Seguridad de la Información (PSI) se orienta hacia la protección de la información y los sistemas, reducción de daños por incidentes y aseguramiento de la continuidad de los servicios, respetando los principios fundamentales de seguridad, que son:

Confidencialidad: Garantizar que sólo personas debidamente autorizadas accedan a la información y sistemas.

Integridad: Asegurar la exactitud de la información y sistemas contra alteración, pérdida o destrucción, ya sea accidental o fraudulenta.

Disponibilidad: Garantizar que la información y sistemas sean accesibles y utilizados según lo requerido por el personal o procesos de negocio.

Resiliencia: Asegurar que los servicios y sistemas puedan recuperarse de fallos o eventos no deseados manteniendo su confiabilidad.

Trazabilidad: Garantizar que las acciones sean imputadas exclusivamente a la entidad correspondiente.

Autenticidad: Garantizar la fuente de los datos y asegurar que los usuarios con acceso a la información sean quienes dicen ser.

Objetivos de la Política de la PSI:

Sus objetivos son:

Definir bases para la protección de la información según criterios de confidencialidad, integridad, disponibilidad, resiliencia, trazabilidad y autenticidad.

Establecer principios generales para la protección de la información y activos asociados.

Incluir pautas que ayuden a cumplir con leyes y regulaciones de seguridad de la información.

Introducir buenas prácticas en seguridad de la información en **Desidedatum Data Company**.

Introducir y referenciar directrices de seguridad de la información y documentos asociados para el tratamiento seguro de la información.

Requisitos Mínimos para cumplir los principios básicos:

Los requisitos mínimos incluyen:

1. Gestión y Evaluación del Riesgo:

- Identificación y evaluación de riesgos.

- Desarrollo de estrategias para mitigar riesgos.

- Monitorización continua de amenazas y vulnerabilidades.

2. Seguridad Ligada al Personal:

- Medidas organizativas y técnicas para gestionar riesgos asociados al factor humano.

- Procedimientos de seguridad durante y después de la contratación.

3. Clasificación de la Información:

- Valoración y clasificación de la información según su importancia y criticidad.

- Adopción de medidas de protección proporcionales al nivel de riesgo.

4. Gestión de Activos:

- Mantenimiento de un inventario de activos de información y relacionados con el LGAI.

- Asignación de responsabilidades a activos específicos.

5. Control de accesos:

- Concesión de acceso basada en la necesidad legítima y autorizada.

- Gestión de identificación y autenticación de usuarios.

6. Seguridad Física y Ambiental:

- Medidas de seguridad para limitar el acceso físico no autorizado.

- Protección contra daños a instalaciones o equipos.

7. Seguridad en las Operaciones:

- Implementación de medidas para asegurar la operatividad de sistemas de producción.

- Inclusión de antivirus, copias de seguridad y gestión de vulnerabilidades.

8. Seguridad en las Telecomunicaciones:

- Protección de redes y comunicaciones.

- Establecimiento de controles según la criticidad de la información.

9. Adquisición, Desarrollo y Mantenimiento de Sistemas:

- Consideración de requisitos de seguridad en proyectos de adquisición y desarrollo.

- Facturación de datos y otros aspectos relacionados con la seguridad.

10. Relaciones con Terceros:

- Establecimiento de medidas contractuales y técnicas para garantizar la seguridad de la información compartida con terceros en función de su criticidad.

11. Gestión de Incidentes:

- Concienciación del personal sobre sus responsabilidades en caso de incidente.

- Gestión eficiente de incidentes para análisis y toma de acciones correctoras.

12. Gestión de la Continuidad del Negocio:

- Planificación para asegurar la continuidad de los servicios.

- Reducción de fallos o interrupciones a niveles aceptables.

13. Cumplimiento Normativo:

- Identificación y actualización de requisitos legales relacionados con la seguridad de la información.

14. Monitorización de la Seguridad de la Información:

- Implementación de métricas y sistemas de seguridad para monitorizar activos de información.

15. Protección de Datos:

- Adopción de medidas técnicas y organizativas para proteger los datos personales.

- Cumplimiento de normativas de seguridad y protección de datos.

Implementación de los principios básicos:

La implementación se basa en principios como seguridad integral, gestión basada en riesgos, vigilancia continua, entre otros. Se aplicarán requisitos mínimos en áreas como organización, análisis de riesgos, gestión de personal, control de accesos, protección de instalaciones, adquisición de productos y servicios de seguridad, etc.

Gestión Documental de los principios rectores:

Se ha desarrollado un procedimiento de gestión y conservación de documentos electrónicos. Además, hay un gestor documental regido por normas internas para la gestión eficiente de documentos del sistema de gestión de seguridad aplicado sobre los sistemas de información.

4.1 Marco normativo

La Política de Seguridad de la Información de **Desidedatum Data Company** está apoyada por un marco normativo alineado con estándares de buenas prácticas y la normativa aplicable en el ámbito de la seguridad de la información. Entre los principales marcos normativos se encuentran:

1. Norma ISO/IEC 27001:2022:

Conocida como "Código de buenas prácticas para la gestión de la seguridad de la información".

Proporciona directrices detalladas para el establecimiento, implementación, mantenimiento y mejora del sistema de gestión de seguridad de la información.

2. ENS RD 311/2022 España:

Regula el Esquema Nacional de Seguridad (ENS).

Establece políticas y requisitos mínimos de seguridad para garantizar la protección de la información en entidades del ámbito público.

La Política de Seguridad de la Información tiene como objetivo alcanzar niveles adecuados de seguridad para diversos tipos de información manejada por **Desidedatum Data Company**, incluyendo información gubernamental, comercial y pública. Para ello, se establecen requisitos de protección específicos, considerando la naturaleza, sensibilidad, requisitos legales y obligaciones comerciales, así como la protección de datos.

El tratamiento de la información de carácter personal se rige por las directrices y las normativas siguientes:

- Política de Protección de Datos Personales Corporativa:

Define las prácticas y principios para el tratamiento de datos personales dentro de la organización.

- Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD):

Conocida como la 'Ley de Protección de datos'.

Regula la protección de datos personales y garantiza los derechos digitales.

- Reglamento (UE) 2016/679 (RGPD):

También conocido como el 'RGPD'.

Establece normas sobre la protección de las personas físicas con respecto al tratamiento de datos personales y a la libre circulación de estos datos.

Desidedatum Data Company se compromete a cumplir con todos los mecanismos y procedimientos indicados en la normativa de privacidad vigente, así como con disposiciones adicionales que puedan completar, desarrollar, modificar o sustituir las leyes mencionadas. La responsabilidad del mantenimiento del marco normativo recae en la organización, que cuenta con un procedimiento para identificar y actualizar la legislación aplicable de manera regular.

Queda recogido en **2024_DDC_149_APO_Avaluació_requisits_legals**

4.2 Organización de la seguridad

La seguridad de la información y los activos que la apoyan es una responsabilidad compartida que involucra a todos los profesionales y terceros que colaboran con **Desidedatum Data Company**. Cada individuo se compromete a participar activamente en esta responsabilidad, actuando de manera ética en la protección de la información. Ello implica cumplir con las obligaciones contractuales relacionadas con la seguridad de la información y garantizar que la información se utilice únicamente para las finalidades establecidas por el negocio.

Trataremos cualquier incidencia de seguridad con la premura que corresponda. Para ello, la empresa ha constituido un Comité de Seguridad de la Información que organizará reuniones puntuales y esporádicas para tratar y resolver estos temas y en caso de ser necesario con el responsable del área que sea afectado por el mencionado incidente y se establecerán los planes de cómo proceder.

4.3 Responsable de seguridad de la Información: Funciones y responsabilidades

El/la responsable de Seguridad es la persona o conjunto de personas encargadas de tomar decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. El ámbito de actuación se limitará exclusivamente a los sistemas de información y servicios de tecnologías de la información y de las comunicaciones bajo la competencia y responsabilidad directa de la organización.

Funciones del Responsable de Seguridad:

1. Definición de Procedimientos de Seguridad:

- Establecer procedimientos de seguridad para garantizar la protección de la información y los servicios electrónicos.

2. Mantenimiento y Verificación del Nivel de Seguridad:

- Garantizar y verificar el nivel adecuado de seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

3. Promoción de Formación y Concienciación:

- Impulsar programas de formación y concienciación en materia de seguridad de la información.

4. Designación de Responsables de Análisis de Riesgos:

- Designar responsables para la ejecución del análisis de riesgos.

- Participar en la declaración de aplicabilidad e identificación de medidas de seguridad.

5. Asesoramiento en Determinación de Categoría del Sistema:

- Colaborar con el Responsable del Sistema y Dirección para determinar la categoría del sistema.

- Proporcionar asesoramiento en aspectos relacionados con la seguridad.

6. Participación en la Elaboración e Implantación de Planes:

- Participar en la elaboración e implantación de planes de mejora de la seguridad.

- Contribuir en la elaboración de planes de continuidad y validarlos cuando sea necesario.

7. Gestión de Revisiones Externas o Internas:

- Gestionar las revisiones externas o internas del sistema de seguridad de la información.

8. Gestión de Procesos de Certificación:

- Gestionar los procesos de certificación del sistema de seguridad de la información.

9. Propuestas y Aprobación de Cambios:

- Elevar a Dirección la propuesta de modificación de la Política de Seguridad de la Información.

- Obtener la aprobación de cambios y otros requisitos del sistema.

El/la Responsable de Seguridad desempeña un papel crucial en la salvaguarda de la información y la protección de los servicios electrónicos, liderando la implementación y mantenimiento de medidas de seguridad efectivas.

4.4 Responsable del sistema: Funciones y responsabilidades

El responsable del Sistema, ya sea de forma directa o a través de recursos propios o contratados, tiene la responsabilidad de desarrollar la implementación concreta de la seguridad en el sistema y supervisar su operación diaria, pudiendo delegar responsabilidades en administradores u operadores bajo su supervisión.

Funciones del Responsable del Sistema:

1. Desarrollo, Operación y Mantenimiento del Sistema:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo especificaciones, instalación y verificación del correcto funcionamiento.

2. Definición de Topología y Gestión del Sistema:

- Definir la topología y la gestión del Sistema de Información, estableciendo criterios de uso y los servicios disponibles.

3. Integración de Medidas de Seguridad:

- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.

4. Suspensión de Acceso o Servicio:

- Paralizar o suspender el acceso a información o prestación de servicio si se identifican deficiencias graves de seguridad.

5. Elaboración de Procedimientos de Seguridad:

- Elaborar procedimientos de seguridad que aseguren el cumplimiento de los requisitos de seguridad.

6. Asesoramiento en Determinación de Categoría del Sistema:

- Prestar asesoramiento al Responsable de Seguridad de la Información para determinar la Categoría del Sistema.

7. Colaboración en Planes de Mejora y Continuidad:

- Colaborar, cuando sea necesario, en la elaboración e implantación de planes de mejora de la seguridad y, si es pertinente, en planes de continuidad.

8. Supervisión de Funciones del Administrador de Seguridad:

- Supervisar las funciones del administrador de seguridad del sistema.

9. Aprobación de Cambios en Configuración:

- Aprobar cambios en la configuración vigente del Sistema de Información.

Cuando la complejidad del sistema lo justifique, el responsable de Sistema tiene la facultad de designar responsables de sistema delegados, los cuales tendrán dependencia funcional directa y serán responsables en su ámbito de todas las acciones que se les delegue. Además, puede delegar funciones específicas en otros roles según sea necesario.

4.5 Responsable del servicio: Funciones y responsabilidades

El responsable del Servicio desempeña un papel primordial en la determinación de los requisitos de los servicios prestados. Su función abarca la definición de niveles de seguridad para cada servicio y la capacidad de establecer requisitos específicos de seguridad. Aquí se describen sus funciones y responsabilidades:

Funciones del Responsable del Servicio:

1. Determinación de Requisitos del Servicio:

- Establecer requisitos de seguridad para los servicios prestados, considerando aspectos específicos y necesidades particulares.

2. Establecimiento de Niveles de Seguridad:

- Determinar los niveles de seguridad adecuados para cada servicio, garantizando la protección de la información y la integridad de los procesos.

3. Normativa de Protección de Datos:

- En el caso de que la información incluya datos de carácter personal, tener en cuenta los requisitos derivados de la normativa interna y la legislación correspondiente sobre protección de datos.

4. Aprobación Formal de Niveles:

- Aprobar formalmente los niveles de seguridad establecidos para cada servicio, asegurando su conformidad con los estándares y requisitos establecidos.

5. Consulta con el Responsable del Sistema:

- Si es necesario, consultar con el Responsable del Sistema antes de definir el nivel de seguridad, buscando su asesoramiento y considerando las especificidades técnicas.

6. Ámbito de Actuación:

- El ámbito de actuación del Responsable del Servicio abarca los sistemas de información y los servicios asociados a su servicio.

7. Cumplimiento Normativo:

- Garantizar el cumplimiento de las normativas y requisitos internos y externos relacionados con la seguridad de la información y la prestación de servicios.

8. Colaboración con otros Responsables:

- Colaborar con otros responsables, como el Responsable del Sistema y el Responsable de Seguridad, para garantizar la coherencia y eficacia de las medidas de seguridad implementadas.

El responsable del Servicio, al tener la responsabilidad de definir los requisitos de seguridad y los niveles adecuados para cada servicio, desempeña un papel fundamental en la protección de la información y la continuidad de los procesos operativos. Su tarea contribuye a garantizar la calidad y seguridad en la prestación de los servicios ofrecidos por la organización.

4.6 Responsable de la Información: Funciones y responsabilidades

El Responsable de la Información es quien crea la información en base a nuestro PSI y los protocolos o procedimientos que se definen para cumplir este PSI con los estándares establecidos.

El Responsable de la Información ejerce un rol central en la garantía de la seguridad de la información, colaborando estrechamente con otros líderes de áreas y coordinando la definición de niveles de seguridad. Su función contribuye a la protección integral de los activos de información de la organización.

4.7 Administrador de la seguridad del sistema: Funciones y responsabilidades

El Administrador de Seguridad, en la estructura organizativa de **Desidedatum Data Company**, desempeña un papel primordial en la implementación y gestión de medidas de seguridad aplicables al sistema de información. Sus funciones abarcan diversas responsabilidades orientadas a garantizar la seguridad integral del sistema. A continuación se detallan sus funciones más significativas:

1. Implementación, Gestión y Mantenimiento de Medidas de Seguridad:

- Liderar la implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información, asegurando su efectividad y adecuación.

2. Gestión de Hardware y Software:

- Gestionar, configurar y actualizar, según sea necesario, el hardware y software que constituyen los mecanismos y servicios de seguridad del sistema de información.

3. Autorizaciones y Privilegios:

- Gestionar las autorizaciones y privilegios concedidos a los usuarios del sistema, monitorizando la actividad para garantizar el cumplimiento de las autorizaciones.

4. Aplicación de Procedimientos Operativos de Seguridad:

- Aplicar los Procedimientos Operativos de Seguridad establecidos para el sistema, asegurando su cumplimiento por parte de los usuarios y otros responsables.

5. Supervisión y Monitoreo:

- Supervisar las instalaciones de hardware y software para garantizar la seguridad, asegurando que cumplen con las autorizaciones pertinentes.

6. Gestión de Eventos de Seguridad:

- Monitorizar el estado de seguridad del sistema mediante herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados.

7. Reporte de Anomalías y Vulnerabilidades:

- Informar al responsable de la Seguridad o al Responsable del Sistema sobre cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

8. Colaboración en Incidentes de Seguridad:

- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su completa resolución.

9. Aprobación de Procedimientos Locales en primera instancia:

- Aprobar los procedimientos locales de control de cambios en la configuración vigente del Sistema, asegurando su coherencia con los requisitos de seguridad.

10. Trazabilidad y Auditoría:

- Asegurar que la trazabilidad, auditoría y otros registros de seguridad se llevan a cabo con regularidad, conforme a la Política de Seguridad establecida.

11. Seguimiento y Reacción ante Alarmas:

- Establecer procedimientos de seguimiento y reacción ante alarmas y situaciones imprevistas, asegurando una respuesta rápida y efectiva.

12. Respuesta ante Incidentes:

- Iniciar el proceso de respuesta ante incidentes, informando y colaborando con el responsable de seguridad en la investigación y resolución de los mismos.

El Administrador de Seguridad desempeña un papel proactivo y estratégico en el mantenimiento de la seguridad del sistema, colaborando estrechamente con otros roles clave en el ámbito de la seguridad de la información.

4.8 Delegado de protección de datos: Funciones y responsabilidades

De conformidad con el artículo 39 del Reglamento General de Protección de Datos (RGPD) y la Política de Protección de Datos Personales, la empresa ejerce de Delegado de Protección de Datos (DPD) a través del correo lopd@desidedatum.com que desempeña un papel crucial en garantizar el

cumplimiento de las normativas de protección de datos. Sus funciones son las siguientes:

1. Informar y Asesorar:

- Proporcionar información y asesoramiento al responsable o al encargado del tratamiento, así como a los empleados involucrados en el tratamiento, sobre las obligaciones establecidas en el RGPD y otras disposiciones de protección de datos.

2. Supervisar el Cumplimiento:

- Supervisar activamente el cumplimiento de las disposiciones establecidas en el RGPD, así como otras regulaciones de protección de datos de la Unión o de los estados miembros. Esto incluye el seguimiento de las políticas del responsable o encargado del tratamiento, la asignación de responsabilidades y la concienciación y formación del personal relacionado con las operaciones de tratamiento.

3. Asesoramiento sobre Evaluación de Impacto:

- Ofrecer asesoramiento solicitado sobre la evaluación de impacto en relación con la protección de datos y supervisar su implementación. La evaluación de impacto es una herramienta importante para evaluar y gestionar los riesgos asociados al tratamiento de datos personales.

4. Cooperar con la Autoridad de Control:

- Colaborar estrechamente con la autoridad de control competente. Esta cooperación implica proporcionar información, responder consultas y abordar cualquier asunto relacionado con el tratamiento de datos personales.

5. Punto de Contacto para la Autoridad de Control:

- Actuar como punto de contacto para la autoridad de control en asuntos relacionados con el tratamiento de datos. El DPD está disponible para consultas y comunicaciones sobre temas específicos relacionados con la protección de datos.

6. Evaluación de Riesgos:

- Ejercer sus funciones teniendo en cuenta los riesgos asociados a las operaciones de tratamiento. Ello implica considerar la naturaleza, alcance, contexto y finalidades del tratamiento de datos personales.

El Delegado de Protección de Datos desempeña un papel fundamental en la promoción de la cultura de protección de datos dentro de la organización,

contribuyendo significativamente a garantizar el respeto de los derechos y libertades de las personas cuyos datos son procesados.

4.9 Punto o persona de contacto: Funciones y responsabilidades

El Punto o Persona de Contacto (POC) desempeña un papel esencial en la gestión de la seguridad de la información y la comunicación con las Administraciones Públicas. Sus funciones incluyen:

1. Representante de la Dirección:

- Actúa como representante de la Dirección de **Desidedatum Data Company**.

- Canaliza y supervisa el cumplimiento de los requisitos de seguridad del servicio proporcionado y las soluciones ofrecidas por **Desidedatum Data Company**.

2. Gestión de Comunicaciones de Seguridad:

- Valorada las comunicaciones relacionadas con la seguridad de la información.

- Gestiona las comunicaciones internas y externas en relación con la seguridad de la información.

3. Gestión de Incidentes:

- Valorada y gestiona los incidentes de seguridad de la información.

- Actúa como punto central para la notificación y resolución de incidentes.

4. Enlace con las Administraciones Públicas:

- Establece y mantiene el enlace con las Administraciones Públicas en asuntos relacionados con la seguridad de la información.

- Asegura el cumplimiento de los requisitos normativos y regulatorios establecidos por las autoridades públicas.

5. Servicios Externalizados:

- En caso de servicios externalizados, garantiza que el proveedor del servicio designe un POC para la seguridad de la información y/o el servicio prestado.

- Colabora con el proveedor externo para garantizar la seguridad de la información tratada.

La figura del POC es crucial para mantener una comunicación efectiva, gestionar incidentes y garantizar el cumplimiento de los requisitos de seguridad, especialmente en situaciones en las que se externalizan servicios o en ausencia temporal del POC designado.

4.10 Sanciones por incumplimiento

El incumplimiento de esta política comporta la aplicación de sanciones laborales, conforme a la normativa laboral o al convenio colectivo vigente. Las sanciones tienen como objetivo garantizar el cumplimiento de las normas y directrices establecidas en la Política de Seguridad de la Información. Algunas de las posibles sanciones laborales incluyen:

1. Advertencia:

- En casos leves de incumplimiento, se puede aplicar una advertencia como medida inicial.

2. Suspensión Temporal:

- En situaciones más graves, se podría imponer una suspensión temporal de las funciones.

3. Sanciones Económicas:

- Se pueden aplicar sanciones económicas proporcionales a la gravedad del incumplimiento.

4. Reasignación de Responsabilidades:

- Dependiendo de la naturaleza del incumplimiento, se podría proceder a la reasignación de responsabilidades.

5. Finalización del Contrato Laboral:

- En casos extremos o reiterados de incumplimiento grave, la empresa podría tomar la decisión de rescindir el contrato laboral.

Es fundamental que todos los profesionales y terceros sujetos a esta política sean conscientes de las posibles sanciones y comprendan la importancia de cumplir con las disposiciones de seguridad de la información. Además, las sanciones se aplicarán de manera justa y proporcional, considerando la gravedad y las circunstancias específicas de cada situación.

4.11 Responsabilidades

La Dirección de Desidedatum Data Company asume las siguientes responsabilidades en relación con la seguridad de la información:

1. Dirección y Apoyo:

- Proporcionar una dirección clara y visible para dar apoyo a las iniciativas de seguridad de la información.

2. Establecimiento de Responsabilidades:

- Aprobar las responsabilidades, procedimientos, controles y medidas necesarios para garantizar la correcta configuración, administración y operación de los sistemas de información y comunicaciones de **Desidedatum Data Company**.

3. Gestión de Incidencias:

- Establecer los medios organizativos, administrativos y técnicos para la notificación, registro, gestión, monitorización y resolución de las incidencias de seguridad.

4. Recursos para Cumplimiento Normativo:

- Disponer de los recursos adecuados para garantizar el cumplimiento de la legislación y regulación vigente en materia de seguridad de la información.

5. Autorización de Acceso a Terceros:

- Autorizar el acceso a los documentos del cuerpo normativo de seguridad de la información por parte de terceros colaboradores que deban conocerlos para el desarrollo de la actividad de negocio.

6. Recursos para Monitoreo:

- Proporcionar los recursos necesarios para la implementación de métricas y sistemas de seguridad que permitan la monitorización de los activos de información de **Desidedatum Data Company**.

Estas responsabilidades buscan garantizar un compromiso activo por parte de la Dirección en el establecimiento, mantenimiento y mejora continua de la seguridad de la información en toda la organización.

Responsabilidades de Todos los Profesionales:

Todos los profesionales de **Desidedatum Data Company** tienen las siguientes responsabilidades en relación con la seguridad de la información:

1. Familiarización con Normativas:

- Familiarizarse con las directrices, normas y procedimientos de seguridad de la información disponibles en el 'Portal de **Desidedatum Data Company**' en el sharepoint de DDC.

2. Conocimiento de Obligaciones:

- Conocer las obligaciones en materia de seguridad de la información asociadas a su puesto de trabajo y aplicar la política, así como las directrices, normas y procedimientos de acuerdo con sus funciones.

3. Formación Obligatoria:

- Realizar las formaciones obligatorias en materia de seguridad de la información establecidas por la empresa.

4. Seguridad de Claves de Acceso:

- Salvaguardar las claves de acceso a los sistemas manteniéndolas en secreto y cambiándolas cuando existan indicios de divulgación.

5. Manipulación de Datos Personales:

- Asegurar que los datos personales se manipulan conforme a las leyes de protección de datos personales vigentes.

6. Cumplimiento Legal:

- Cumplir con la legislación vigente que afecte al desarrollo de sus funciones de negocio.

7. Uso de Activos y Sistemas:

- Utilizar únicamente los activos y sistemas de información, así como cualquier tipo de TIC, proporcionados o previamente homologados por la subárea de Sistemas y Seguridad de la información.

8. Reporte de Incidentes:

- Reportar todos los incidentes de seguridad que afecten a información confidencial directamente a Helpdesk, incluyendo el Departamento de Seguridad.

Estas responsabilidades buscan involucrar a todos los profesionales en la protección de la información y fomentar una cultura de seguridad en toda la organización.

Responsabilidades de Terceros Colaboradores (Proveedores):

Los terceros colaboradores o proveedores de **Desidedatum Data Company** tienen responsabilidades específicas en relación con la seguridad de la información. Estas responsabilidades incluyen:

1. Conocimiento y Cumplimiento de la Política de Seguridad:

- Conocer, asumir y cumplir con la Política y el resto del cuerpo normativo de seguridad que los aplique.

- Mantener el secreto profesional y la confidencialidad de los datos tratados en su entorno laboral.

2. Firma de Contrato de Confidencialidad:

- Firmar un contrato de confidencialidad y no divulgación de la información antes de acceder a cualquier tipo de información.

3. Reporte de Incidencias:

- Reportar cualquier incidencia de seguridad en Helpdesk con copia al Departamento de Seguridad (seguridad@desidedatum.com).

- En casos donde la incidencia afecte a datos personales, también se debe informar al Delegado de Protección de Datos (lopd@desidedatum.com).

Además, la Dirección de **Desidedatum Data Company** destaca la importancia de que los profesionales promuevan el conocimiento y el cumplimiento del cuerpo normativo de seguridad dentro de **Desidedatum Data Company**. Se entenderá a todos los profesionales a participar activamente en la mejora continua de la seguridad de la información del Grupo mediante la presentación de propuestas al Departamento de Seguridad a través del correo electrónico (seguridad@desidedatum.com).

Definiciones

Se han proporcionado algunas definiciones clave relacionadas con la política de seguridad de la información de **Desidedatum Data Company**. Aquí están las definiciones:

- **Desidedatum Data Company**: Consultar la Política de políticas y procedimientos.

- **Activo de Información**: Cualquier componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente, con consecuencias para la organización. Incluye información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

- **Custodio del Activo de Información**: Persona responsable de implementar las políticas, procedimientos, medidas y controles de seguridad establecidos por el propietario del riesgo y el Departamento de Seguridad.

- **Incidencia de Seguridad de la Información**: Acontecimiento que puede poner en riesgo la seguridad de la información, constituyendo un incumplimiento de los requisitos de confidencialidad, integridad y/o disponibilidad de los activos de información, y que, según su naturaleza y alcance, puede causar daños considerables a la empresa.

- **Información Confidencial**: Información marcada para el uso exclusivo de un grupo reducido de usuarios, con controles estrictos para mantener su confidencialidad y cuya difusión ilícita está expresamente prohibida, ya que puede resultar en un impacto negativo elevado para **Desidedatum Data Company**.

- **Propietario de un Activo de Información**: Persona responsable del activo de información y de la información contenida en el mismo, garantizando su protección y seguridad siguiendo procedimientos homologados y consultando al Departamento de Seguridad cuando sea necesario.

- **Responsable de un Activo de Información**: Profesional responsable de determinar el nivel de clasificación del activo, el grado de seguridad, el uso del activo y proporcionar autorizaciones de permisos necesarias. Puede delegar algunas funciones mediante procedimientos formales, pero sigue siendo el responsable último del activo.

- **TI (Tecnologías de la Información) y TIC (Tecnologías de la Información y Comunicación)**: Todos los recursos, herramientas y programas utilizados para procesar, administrar y compartir información mediante soportes tecnológicos como ordenadores, teléfonos móviles, televisores, reproductores audiovisuales, entre otros.

- **Usuario/a**: Profesional que utiliza un activo de información.

5. Vigencia y revisión de la Política

Este documento entrará en vigor al día siguiente de su aprobación y reemplazará cualquier política existente con el mismo objeto hasta la fecha de aprobación.

La política deberá ser revisada al menos una vez al año y siempre que haya cambios significativos en la organización. Para ello, la subárea de Sistemas y Seguridad de la Información evaluará si el contenido de la política continúa siendo adecuado para cumplir con los objetivos, estrategias y necesidades establecidos por **Desidedatum Data Company**. En caso necesario, se realizarán modificaciones.

Durante la revisión periódica de la política, se tomarán en cuenta las "lecciones aprendidas" durante el período transcurrido desde la última revisión. Además, se implementarán medidas para la detección, prevención y corrección de amenazas y vulnerabilidades identificadas. La revisión de la política puede llevar a la actualización de directrices, normas y procedimientos de seguridad de la información.

Próxima revisión: 07/2025

DesideDatum