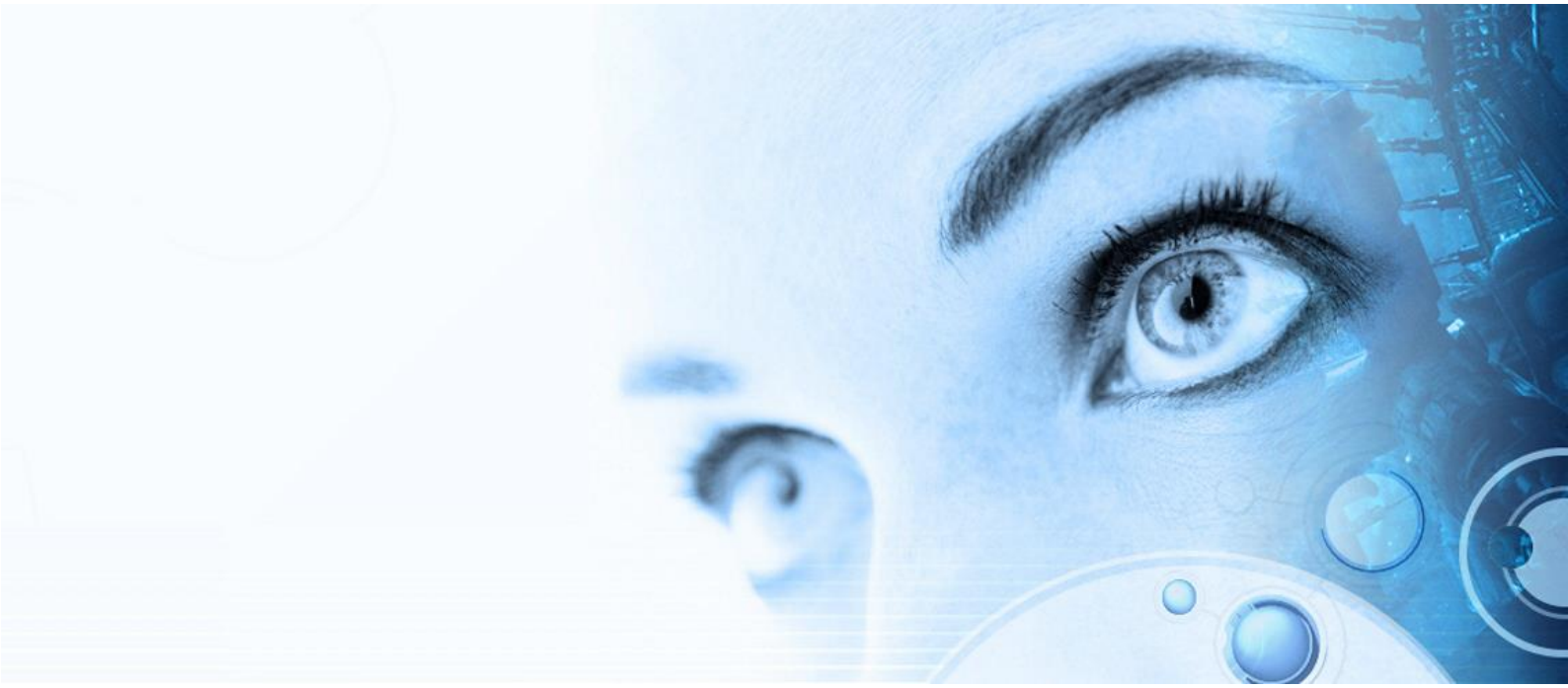
VIRTUALDESK



POLÍTICA DE SEGURIDAD

Versión: 4.0

Fecha de aprobación: 15/06/2023

Estado: Aprobado

Control de Versiones

Versión	Autor	Descripción	Fecha Entrega
1.0	Equipo consultor	Versión inicial	Marzo 2021
2.0	Comité de seguridad	Revisión	Abril 2021
3.0	Comité de seguridad	Revisión para auditoria ENS	Mayo 2021
4.0	Comité de seguridad	Actualización nueva ENS	Junio 2023

Responsabilidades

Acción	Nombre	Compañía	Fecha
Realizado por:	Equipo Consultor	Virtual Desk	Junio 2023
Revisado por:	Francisco Manzano	Virtual Desk	Junio 2023
Aprobado por:	Julio Martín Emilio Martín	Virtual Desk	Junio 2023

Documentos de referencia

Documento	Comentarios
Artículo 12	Política de Seguridad

Calificación del documento

Difusión		Seguridad	
IN1 Interna	**IN1**	**NL1: General**	**NL2**
IN2 Clientes		**NL2: Restringido**	
IN3 Exterior		**NL3: Confidencial**	

Índice

1. Introducción

Virtual Desk es una empresa de tecnología, con más de 25 años de experiencia, especializada en el desarrollo e integración de soluciones innovadoras, con un amplio conocimiento de los retos y necesidades de las administraciones en el ámbito de la movilidad inteligente y de la gestión de procesos de servicios sociales, así como de soluciones adaptadas a éstos, en base a la experiencia adquirida en el desarrollo de proyectos tanto en administraciones municipales como autonómicas y en la Administración General del Estado.

Está altamente comprometida con la innovación y la calidad de servicio.

Es partner estratégico de IBM en materia de Soluciones para Administración Pública y para proyectos de Big Data & Analytics.

Acompañamos a las organizaciones y organismos públicos en el reto de abordar su transformación digital, facilitándoles la adopción inteligente de tecnologías capaces de optimizar sus procesos, transformar sus modelos de operación y redefinir sus modelos de negocio, mediante:

- Una propuesta integral de soluciones digitales
- Enfocada a la mejora de la relación con sus ciudadanos y entorno
- Con foco en avanzar hacia la excelencia y eficiencia en la gestión de sus negocios y de su actividad de prestación de servicios públicos.

Tenemos la experiencia y las capacidades necesarias para ser el partner estratégico de nuestros clientes en su camino hacia la Transformación Digital, que requiere una revisión profunda de sistemas de información, modelos de negocio, procesos, personas e infraestructuras, con un enfoque centrado en el ciudadano y en la mejora operacional.

Dentro de los servicios ofrecidos, la seguridad de la Información es uno de los puntos principales en el modelo de Gobierno IT que Virtual Desk tiene. Para ello en el año 2019 ya obtuvo las certificaciones tanto en la norma UNE-EN-ISO 9001:2015 como en la UNE-ISO/IEC 27001:2014.

Estableciendo así un Sistema integrado de Calidad y seguridad de la información en la manera de construir software y ofrecer servicios a las organizaciones con las que trabaja.

2. Marco normativo

El marco normativo en materia de seguridad de la información en el que Virtual Desk desarrolla su actividad, esencialmente, es el siguiente:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- RD 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- ENS. Artículo 12. Organización e implantación del proceso de seguridad.

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (reglamento General de Protección de Datos), de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.
- Ley 34/2002, de 11 de julio, de Servicios de la Información de Comercio electrónico, LSSICE.
- Guía de Seguridad de las TIC CCN-STIC 805 ENS. Política de seguridad de la información.
- Guía de Seguridad de las TIC CCN-STIC 801 ENS. Responsabilidades y funciones.
- El convenio colectivo aplicable, correspondiente a “Empresas de consultoría, y estudios de mercado y de la opinión pública”.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).
- UNE-EN-ISO 9001, UNE-EN_ISO_14001, UNE-ISO-IEC_27001, UNE ISO 20000, ISO 33000

3. Alcance

El alcance de la presente política está en los sistemas, personas, y proveedores que intervienen en el **Ciclo de vida del desarrollo, implementación y mantenimiento de la Plataforma SOCYAL.**

4. Organización e implantación del proceso de seguridad (art. 13)

Esta “Política de Seguridad de la Información” es efectiva desde su entrada en vigor el día 15 de junio de 2023 por Virtual Desk

La Política es revisada por el Responsable de Seguridad de la Información a intervalos planificados, sin exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización, comunicándose de forma efectiva.

Los cambios sobre la Política de Seguridad de la Información serán aprobados por la Dirección de Virtual Desk. Cualquier cambio sobre la misma deberá ser difundido para conocimiento de toda la Organización.

La dirección de la empresa es consciente del valor de la información y está profundamente comprometida con la política descrita en este documento.

5. Principios y Directrices

Virtual Desk depende de los sistemas TIC[1] para alcanzar sus objetivos.

Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad o trazabilidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

5.1. Misión y objetivos

Se desarrollarán, al menos los siguientes objetivos:

a) Utilización de recursos TIC corporativos, tales como el correo electrónico, el acceso a Internet, el equipamiento informático y de comunicaciones.

b) Gestión de activos de información inventariados, categorizados y asociados a un responsable.

c) Mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Seguridad física, de forma que los activos de información serán emplazados en áreas seguras, protegidos por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

e) Seguridad en la gestión de comunicaciones y operaciones, de manera que la información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

f) Control de acceso, limitando el acceso a los activos de información por parte de usuarios, procesos y sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información contemplando los aspectos de seguridad de la información en todas las fases del ciclo de vida de dichos sistemas.

h) Gestión de los incidentes de seguridad implantando mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

[1] Tecnologías de Información y Comunicaciones.

i) Gestión de la continuidad implantando mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y manteniendo la continuidad de sus procesos de negocio.

5.2. Prevención

Para defenderse de las amenazas, los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema.

Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en las ofertas, y en pliegos de licitación para proyectos de TIC. Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 7 del ENS.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

5.3. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continuada para detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo establecido en el art. 8 y art. 9 del ENS.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

5.4. Respuesta

Virtual Desk y sus departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones con los Equipos de Respuesta a Emergencias (CERT[2]).

[2] Computer Emergency Response Team: Conjunto de personas responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

5.5. Recuperación

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

6. Organización de la seguridad

La implantación de la Política de Seguridad en Virtual Desk requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado.

Como parte de la Política de Seguridad de la Información, los principales roles quedan identificados y detallados del modo siguiente:

- Responsable de Seguridad: ***Julio Martin Parro***
- Responsable de la Información: ***Francisco Manzano Pérez***
- Responsable del Servicio de Desarrollo de Producto: ***Oscar García***
- Responsable de Sistemas: ***Emilio Martin Parro***

En los siguientes apartados se especifican las funciones atribuidas a cada uno de estos roles.

6.1. Comités: Funciones y Responsabilidades

La Seguridad de la Información es una responsabilidad organizativa que es compartida con el Director General. En consecuencia, éste promueve la composición de un Comité de Seguridad de la Información, en aras de establecer una vía definida y de apoyo a las iniciativas de seguridad.

Dicho Comité está compuesto por cada una de las figuras anteriormente mencionadas y por un presidente que será responsable último de las decisiones adoptadas y que dirigirá las reuniones del Comité de Seguridad, informando, proponiendo y coordinando las actividades y decisiones.

Esta función de presidente inicialmente recae en le Responsable de Seguridad.

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Revisión de la Política de Seguridad de la Información y de las responsabilidades principales y propuesta de aprobación al Órgano de Gobierno.
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinadas a garantizar la Seguridad de dichos activos.
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de aspectos tales como:
    - Principales incidencias en la Seguridad de la Información.

- Elaboración y actualización de planes de continuidad.
- Cumplimiento y difusión de las Políticas de Seguridad.

6.2. Responsable de Seguridad

Es el responsable de la definición, coordinación y verificación de cumplimiento de los requisitos de seguridad de la información definidos en los objetivos estratégicos.

Las funciones del responsable de Seguridad de la Información son las siguientes:

- Responsable de la Seguridad es la persona designada por la Dirección de la Organización.
- Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- Trabajar para conseguir una total seguridad de los datos de la empresa, así como la privacidad de estos.
- Supervisar, controlar y administrar el acceso a la información de la empresa, y de sus trabajadores.
- Elaborar un conjunto de medidas de respuesta ante incidentes de seguridad relacionados con la información, incluyendo la recuperación ante desastres.
- Garantizar el cumplimiento de la normativa relacionada con la seguridad de la información.
- En caso de servicios externalizados, la responsabilidad última la tiene siempre la Organización destinataria de los servicios, aun cuando la responsabilidad inmediata pueda corresponder (vía contrato) a la organización prestataria del servicio.
- Mantener la seguridad de la información manejada y de los servicios prestados por los
- Sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la
- Política de Seguridad de la Información de la organización.
- Promover la formación y concienciación en materia de seguridad de la información.
- Garantizar el buen uso del equipamiento informático
- dentro de su ámbito de responsabilidad.
- Supervisar y coordinar al equipo encargado de llevar a cabo las medidas de respuesta en caso de brechas de seguridad.
- POC (Persona de contacto de seguridad de la información) Se responsabilizará de la seguridad con los Clientes, en los que presta servicio Virtual Desk.
- Realizar operaciones de seguridad para luchar contra el fraude y el robo de información.

- Diseñar del Plan de formación, en el ámbito del ENS, para las personas de Virtual Desk que prestan servicios en proyectos de AA.PP.

6.3. Responsable de Sistemas

Es responsable de asegurar la ejecución de medidas para protección de los activos y servicios de los sistemas de información que soportan la actividad de Virtual Desk.

Las funciones del Responsable de Sistemas de la Información son las siguientes:

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el proceso de análisis y gestión de riesgos en el Sistema.
- Determinar la categoría del sistema y determinar las medidas de seguridad que deben aplicarse Elaborar y aprobar la documentación de seguridad del Sistema.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.

6.4. Responsable de la Información

Es responsable de asegurar la integridad, autenticidad, y trazabilidad de toda la información que soportan la actividad de Virtual Desk.

Las funciones del Responsable de la Información son las siguientes:

- Aceptar los riesgos residuales respecto de la información, calculados en el análisis de riesgos.
- Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, se puede recabar una propuesta al Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.
- Determinar los requisitos de la información tratada.
- Velar por la seguridad de la información en sus diferentes vertientes: protección física, protección de los servicios y respeto de la privacidad.
- Estar al tanto de cambios normativos (leyes, reglamentos o prácticas sectoriales) que afecten a la Organización

- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural

6.5. Responsable del Desarrollo del producto

Es responsable de asegurar todo el proceso de desarrollo que soportan la actividad de Virtual Desk.

Las funciones del Responsable del Desarrollo son las siguientes:

- Tiene la facultad de establecer los requisitos, en materia de seguridad, de los servicios prestados relacionados con el desarrollo de la Plataforma SOCYAL
- Describe los requisitos de Desarrollo
- Vela por el cumplimiento de las metodologías de desarrollo de Virtual Desk, así como de los requisitos de seguridad del producto
- Determina los niveles de seguridad del servicio.

6.6. Delegado de Protección de Datos (DPD)

Es responsable de asegurar todo el proceso normativo que soportan la actividad de Virtual Desk.

Las funciones del DPD son las siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.
- Desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Además, el responsable del sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de seguridad, antes de ser ejecutado.

6.7. Procedimientos de Designación

El responsable de Seguridad de la Información será nombrado por el Órgano de Gobierno a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El Departamento responsable de un servicio que se preste electrónicamente de acuerdo con la Ley 11/2007 designará al responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

6.8. Difusión, actualización y revisión de la política de seguridad de la información

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de esta.

La Política será aprobada por el Órgano de Gobierno y será difundida para que la conozcan todas las partes afectadas.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos.

La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

7. Datos de carácter personal

La Política de Protección de Datos y el Manual de Medidas de Seguridad definido en el documento "***VD_(ORG)_Documento de seguridad.V2"*** al que tendrán acceso sólo las personas autorizadas, identifican los responsables de los tratamientos de datos personales, detallan estos tratamientos y exponen las medidas de seguridad correspondientes.

Todos los sistemas de información de Virtual Desk se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el Documento de Seguridad.

En aplicación del principio de responsabilidad proactiva establecido en el Reglamento General de Protección de Datos (GDPR), y la nueva LOPD, las actividades de tratamiento de datos de carácter personal se integrarán en la categorización de sistemas del Esquema Nacional de Seguridad, considerando las amenazas y riesgos asociados a este tipo de tratamientos.

Se aplicará, asimismo, cualquier otra normativa vigente en materia de protección de datos de carácter personal.

8. Análisis y Gestión de los Riesgos (Art.14)

Se realizará un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis será la base para determinar las medidas de seguridad que se deben adoptar, además de los mínimos establecidos según lo previsto en el artículo 7 y 14 del BOE, se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.
- Cuando haya un incidente de seguridad relacionado con la normativa LOPDGDD
- Cuando haya una brecha de seguridad relacionada con la información tratada de un usuario según la normativa LOPDGDD.

Los criterios de evaluación de riesgos se especificarán en la metodología de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave. Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios, o repercuta a dicha información tratada durante el servicio.

Los criterios de evaluación de riesgos se especificarán en la metodología de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas. Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave. Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios de Virtual Desk en los Clientes.

El propietario de un riesgo debe ser informado de los riesgos que afectan a su propiedad y del riesgo residual al que está sometida. Cuando un sistema de información entra en operación, los riesgos residuales deben haber sido aceptados formalmente por su correspondiente propietario.

9. Gestión de Personal (Art.15)

El personal, propio o ajeno, relacionado con los sistemas de información sujetos a lo dispuesto en este real decreto, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad.

Su actuación, deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en el documento Normativa de Seguridad que será aprobada por la dirección de Virtual Desk. Se difundirá a toda la Organización, siendo obligatorio su difusión para cada incorporación en Virtual Desk.

10. Profesionalidad (Art. 16)

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

Las entidades del ámbito de aplicación de este real decreto exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

Virtual Desk determinará los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

11. Autorización y control de los accesos (Art. 17)

El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación de este real decreto deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Los privilegios de acceso de un recurso (persona) al sistema de información de Virtual Desk, quedan restringidos por defecto al mínimo necesario para el desarrollo de sus funciones.

El sistema de información de Virtual Desk se mantendrá siempre configurado, de tal manera que evite que un recurso (persona) pueda acceder accidentalmente a recursos con derechos distintos de los autorizados.

12. Protección de las instalaciones (Art. 18)

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos, sin perjuicio de lo establecido en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

13. Adquisición de productos de seguridad y contratación de servicios de seguridad (Art. 19)

En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información del ámbito de aplicación de este real decreto, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional (en adelante, CCN), constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas por este organismo y en función del uso previsto del producto o servicio concreto dentro de sus competencias, determinará los siguientes aspectos:

a) Los requisitos funcionales de seguridad y de aseguramiento de la certificación.

b) Otras certificaciones de seguridad adicionales que se requieran normativamente.

c) Excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el artículo 16.

14. Mínimo privilegio (Art. 20)

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados.

c) Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

15. Integridad y actualización del sistema (Art. 21)

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

16. Protección de la información almacenada y en tránsito (Art. 22)

En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

17. Prevención ante otros sistemas de información interconectados (Art. 23)

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, tal y como se definen en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

18. Registro de la actividad y detección de código dañino (Art. 24)

Con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información, garantizando y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, los sujetos comprendidos en el artículo 2 podrán, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

19. Incidentes de seguridad (Art. 25)

La entidad titular de los sistemas de información del ámbito de este real decreto dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente y, en caso de tratarse de un operador de servicios esenciales o de un proveedor de servicios digitales, de acuerdo con lo previsto en el anexo del Real Decreto 43/2021, de 26 de enero , por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

20. Continuidad de la actividad (Art. 26)

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

21. Mejora continua del proceso de seguridad (Art. 27)

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

22. Terceras partes

Cuando Virtual Desk utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

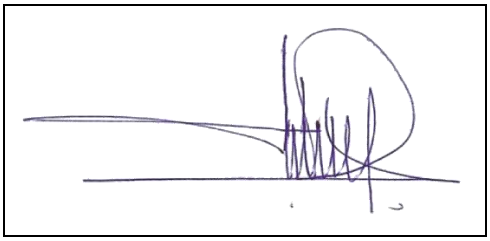
Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

23. Aprobación

Documento: VD_Politica de Seguridad Firmado:

Estado: Aprobado

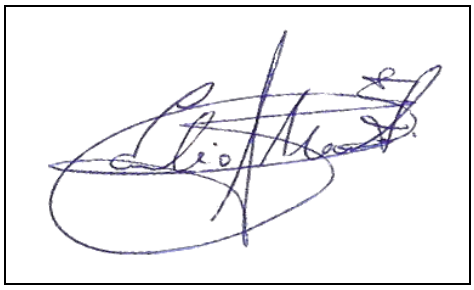
Fdo. Julio Martín Parro (CEO)



Documento: VD_Politica de Seguridad Firmado:

Estado: Aprobado

Fdo. Emilio Martín Parro (CIO)



VIRTUAL DESK
Pº de la Castellana, 151 - 2ºB - 28046 Madrid
Tlfno: 915 980 460 - Fax: 910 811 511
C.I.F.: B80618085
www.virtualdesk.es