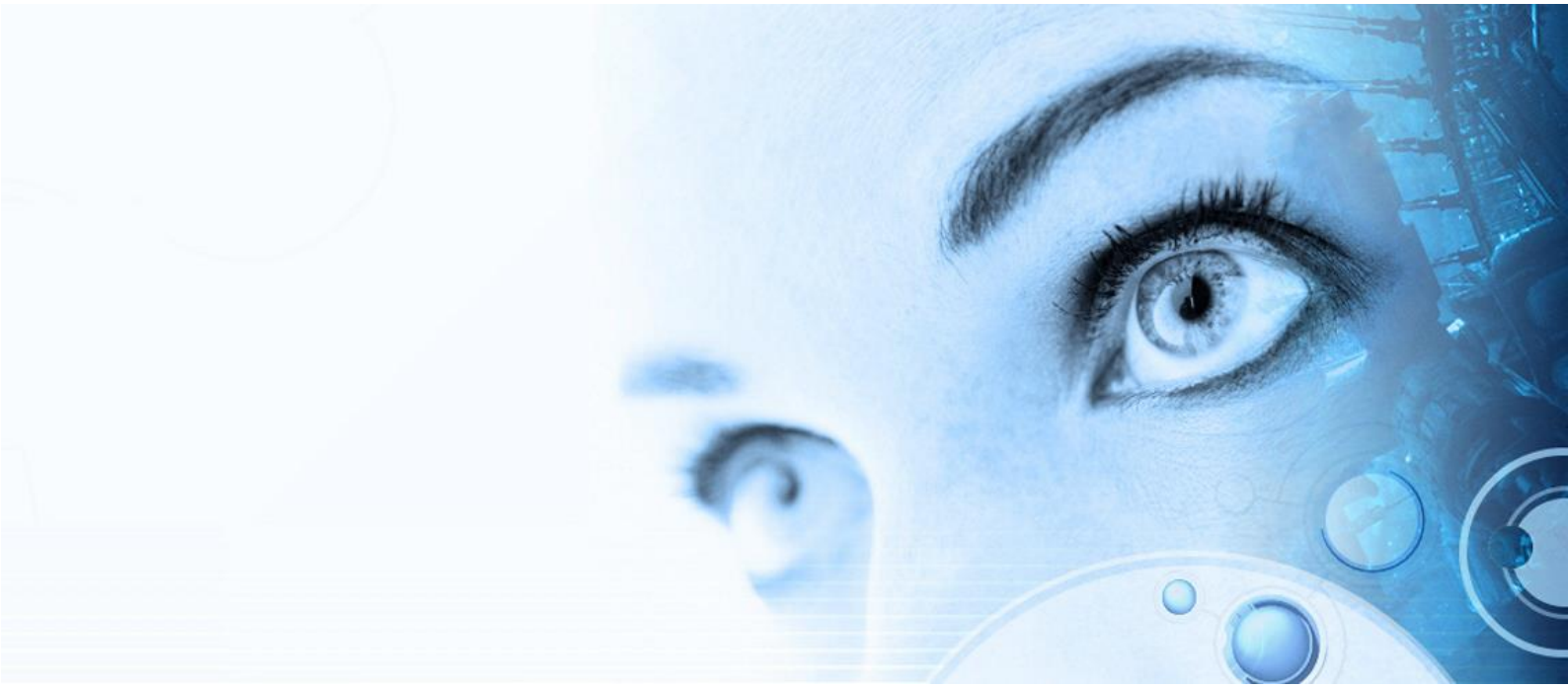
VIRTUALDESK



POLÍTICA DE SEGURIDAD (ENS)

Versión: 3.0

Fecha de aprobación: 25/05/2021

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

Responsabilidades

Acción	Nombre	Compañía	Fecha
Realizado por:	Equipo Consultor	Virtual Desk	Marzo 2021
Revisado por:	Francisco Manzano Oscar García Javier Bosque	Virtual Desk	Abril 2021
Aprobado por:	Julio Martín Emilio Martín	Virtual Desk	Mayo 2021

Documentos de referencia

Documento	**Comentarios**
Manual Integrado de Calidad y Seguridad de la Información	
Esquema Nacional 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 y en 2021 la ISO 33000 y en el modelo de procesos del ciclo de vida del software de acuerdo con la norma ISO/IEC 12207:2017 conforme al “Modelo de Madurez de Ingeniería de software versión 2.0 (MMIS V.2)”: NIVEL 3.

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 de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.
- 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 y por el que se deroga la Directiva 95/46/CE.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de comercio electrónico.
- Ley 59/2003, de 19 de diciembre, de firma electrónica
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Real Decreto 4/2010, de 8 de enero, por el **que** se regula **el Esquema Nacional de Interoperabilidad** en el ámbito de la Administración Electrónica.
- Guías CCN-STIC, 802, 807, 808, 809 y 825.
- Instrucciones Técnicas de Seguridad de conformidad con el Esquema Nacional de Seguridad (Resolución de 13 de octubre de 2016 de la Secretaría de Estado de Administraciones Públicas) y de Auditoría de la Seguridad de los Sistemas de Información (Resolución de 27 de marzo de 2018 de la Secretaría de Estado de Función Pública).
- UNE - ISO/IEC 27002:2013 Código de buenas prácticas para la Gestión de la Seguridad de la información.
- UNE - ISO/IEC 27001:2013 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.
- UNE-EN-ISO 9001:2015 Sistemas de gestión de la calidad.

3. Alcance

Aunque en VIRTUAL DESK existe una política de seguridad implementada bajo la normativa EN-ISO/IEC 27001:2014 cuyo alcance afecta a todos los sistemas, trabajadores y proveedores que tengan relación con la empresa.

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. 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.

[1] Tecnologías de Información y Comunicaciones.

4.1. 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.

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.

4.2. 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 al 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.

4.3. 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.

4.4. 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 (CERT2).

4.5. 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.

5. 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 Martín Parro***
- Responsable de la Información: ***Francisco Manzano Pérez***
- Responsable del Servicio de Desarrollo de Producto: ***Oscar García Farré***
- Responsable de Sistemas: ***Emilio Martín Parro***

En los siguientes apartados se especifican las funciones atribuidas a cada uno de estos roles. Estas funciones están actualizadas en el manual de Funciones de VIRTUAL DESK VD_(MAN)_Manual de Funciones.

5.1. Comité de Seguridad: Funciones y Responsabilidades

La Seguridad de la Información es una responsabilidad organizativa que es compartida con el presidente. 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.

[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.

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.

5.2. 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:

- Supervisar y velar por el cumplimiento de la normativa legal aplicable
- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de VIRTUAL DESK.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:
    - La estrategia de seguridad de la información definida por el Comité de Seguridad.
    - Las normas y procedimientos contenidos en la Política de Seguridad de la Información de VIRTUAL DESK y normativa de desarrollo.
- Supervisar los incidentes de seguridad producidos en VIRTUAL DESK.
- Difundir en VIRTUAL DESK las normas y procedimientos contenidos en la Política de Seguridad de la Información y normativa de desarrollo, así como las funciones y obligaciones en materia de seguridad de la información.
- Supervisar y colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables en materia de protección de datos personales y de seguridad de la información.
- Asesorar en materia de seguridad de la información a las diferentes áreas operativas de VIRTUAL DESK.

5.3. 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 de Información durante el ciclo de vida, especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Seleccionar y establecer las funciones y obligaciones a los Responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos de VIRTUAL DESK conforme a la estrategia de seguridad definida.
- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en VIRTUAL DESK.
- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.
- 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 la Seguridad, antes de ser ejecutada.

5.4. Responsable de la Información

- Establece los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación sobre protección de datos.
- Determina los niveles de seguridad de la información.

5.5. Responsable del Desarrollo del producto

- 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.

5.6. 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 a la Ley 11/2007 designará al responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

5.7. 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 la misma.

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.

5.8. Estructuración de la documentación

Será el responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de la documentación generada. La documentación sobre la que se soporta esta política estará compuesta por un conjunto de Normas, guías y procedimientos que ayudarán a los usuarios en el desarrollo de sus tareas.

Esta documentación se encuentra dentro del sistema de documentación de VIRTUAL DESK en la herramienta DOCUO donde existen tres carpetas:

- MULTISO; que incluye la documentación relativa a los sistemas de gestión ISO 9001 y 27001
- ISO 33000, que incluye la documentación relativa a la documentación catalogada de nivel 3
- ENS; documentación relativa al sistema de información de la Plataforma Socyal bajo Esquema Nacional de Seguridad

6. Datos de carácter personal

La Política de Protección de Datos y el Manual de Medidas de Seguridad 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.

7. Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

Este análisis 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.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información que manejados y los diferentes servicios prestados.

El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

La gestión de riesgos quedará documentada en el informe de Análisis y gestión de riesgos[3].

8. Obligaciones del personal

Todos los miembros de VIRTUAL DESK tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de VIRTUAL DESK atenderán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de VIRTUAL DESK, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinares que procedan, sin prejuicio de las responsabilidades legales correspondientes.

[3] Se puede encontrar tal Informe en el Sistema de Gestión de Esquema Nacional de Seguridad.

9. 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.

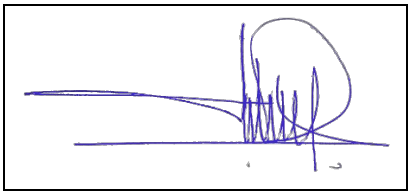
Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables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

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

Documento: Normativa de Seguridad ENS Firmado:

Estado: Aprobado

Fdo. Julio Martín Parro (CEO)



Documento: Normativa de Seguridad ENS Firmado:

Estado: Aprobado

Fdo. Emilio Martín Parro (CIO)