INTERFACE SAFEACCESS	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

FECHA:	25/05/2022	**EDICIÓN:**	**2**

Índice

INTERFACE SAFEACCESS	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

FECHA:	25/05/2022	EDICIÓN:	2

Política desarrollada según anexo II, 3.1 Política de seguridad [org.1] del RD 3/2010.

1. Marco normativo

Nº	Legislación
1	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 (Reglamento general de protección de datos)
2	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
3	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
4	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
5	Real Decreto 1777/2004, de 30 de julio, por el que se aprueba el Reglamento del Impuesto sobre Sociedades
6	Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores
7	Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal
8	Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones
9	Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (Deroga ley 59/2003)
10	Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
11	Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. (Deroga RD 3/2010)

2. Responsabilidades y organización de la seguridad

a. Comité STIC (Seguridad TIC)

Las actividades TIC se coordinan por medio del comité STIC. Este comité está compuesto de personal técnico de los diferentes departamentos para la toma de las decisiones.

El comité de seguridad TIC estará formado por:

CARGO	NOMBRE
Dirección, Responsable de la información	Jordi Mateu i Rosell
Dirección Tecnológica	Felipe Ros Torralba
Responsable Operaciones	Francisco Ponce

Responsable del servicio	Felipe Ros Torralba
Responsable de la Seguridad	Marc Rué i Palau

El Director preside el Comité STIC y es el principal responsable de:

- Usar el voto de calidad, para acordar las decisiones oportunas, cuando no se produce un acuerdo dentro del equipo.
- Implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI)
- Asignar los recursos necesarios y aprobar el presupuesto
- Asignar y comunicar los roles, concretamente de los propietarios de los riesgos de seguridad de la información y los riesgos de calidad.

Otros de los roles de gran relevancia dentro del sistema de seguridad de la información son:

CARGO	NOMBRE	RESPONSABILIDADES
Administrador sistemas TIC	Felipe Ros Torralba	Responsable de la implementación, configuración y mantenimiento de los servicios de seguridad relacionados con las TIC
Operadores sistemas TIC	Marc Rué Palau	Equipo de continuidad. Son los responsables de la operación diaria de los servicios de seguridad relacionados con las TIC
	Francisco Ponce	

b. Funciones y responsabilidades

Comité de STIC

- Establecer, revisar y aprobar el alcance del SGSI, además de la política de seguridad de la información.
- Asegurar que las políticas de seguridad de la información, los procesos, procedimientos y leyes y regulaciones reflejan los requisitos del negocio y están alineados con los requerimientos de las partes interesadas, tanto internas como externas.
- Además de establecer, revisar y aprobar los objetivos del SGSI y comprobar si están eficazmente implementado y mantenido.
- Monitorizar los cambios importantes en la seguridad de la información.
- Revisar los incidentes de seguridad de la información y acordar las acciones necesarias, si procede.
- Aprobar las iniciativas más importantes para mantener la seguridad de la información y el nivel de calidad establecido.
- Realizar Revisiones por la Dirección a intervalos planificados.
- Asegurar que el personal está concienciado de la importancia de cumplir los requisitos de seguridad, los requisitos legales y regulatorios, las obligaciones

contractuales, los requisitos de calidad, los niveles de calidad y los acuerdos de nivel de servicio.

Responsable de la Información

- Tiene la facultad de establecer 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 correspondiente sobre protección de datos
- Determina los niveles de seguridad de la información.

Responsable del Servicio

- Tiene la facultad de establecer los requisitos, en materia de seguridad, de los servicios prestados.
- Determina los niveles de seguridad del servicio.

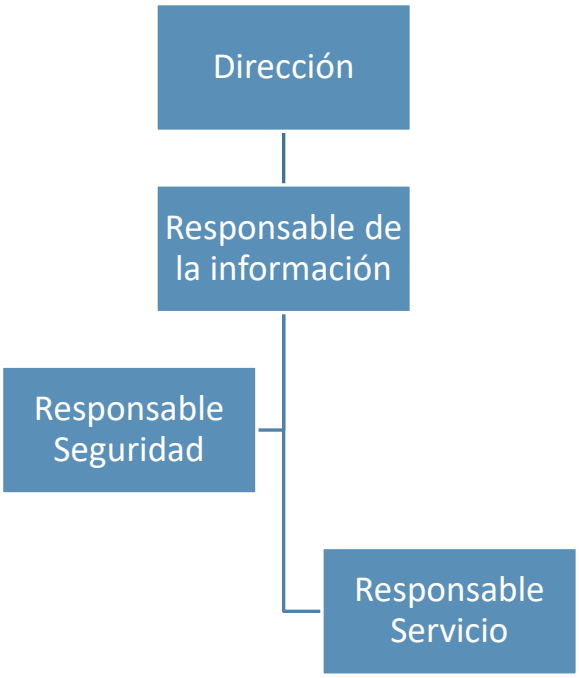
Responsable de Seguridad

Responsable de la definición, coordinación y verificación de cumplimiento de los requisitos de seguridad de la información definidos de acuerdo a los objetivos.

Las funciones del Responsable de Seguridad de la Información son:

- Coordinar y controlar las medidas de seguridad de la información y de protección de datos.
- 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.
    - Supervisar los incidentes de seguridad.
    - Difundir entre el personal de la empresa las normas y procedimientos contenidos en el sistema de gestión de la Seguridad de la Información, 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 la empresa.

Dependencias de los roles



3. Designación y renovación de los roles de seguridad

Dirección es la máxima responsable de designar los diferentes roles de seguridad. Esta designación se realizará formalmente con la aprobación de la presente política. El original firmado por Dirección será archiva por el Responsable de Seguridad.
El organigrama establecido reflejará estas designaciones.

La designación se renovará en los casos siguientes:

- Baja a medio o largo plazo del personal designado.
- Personal causa baja indefinida de la empresa
- Falta de competencias
- Criterio de Dirección atendiendo a razones de gestión de RRHH y/o estratégicas.

4. Gestión del riesgo

Los activos sujetos a esta política de seguridad deberán ser sometidos a un análisis del riesgo, evaluando posibles amenazas y a que riesgos pueden estar expuestos. Este análisis se repetirá regularmente, al menos una vez al año o se reporten vulnerabilidades graves.

5. Recursos

Para la aplicación efectiva de la Política de Seguridad de la Información en la compañía, la Dirección dotará de los recursos necesarios para su buen desarrollo, tanto en las actividades de implantación como de operación y mejora de dicha política y de los controles de seguridad de la información que en cada momento se establezcan.

La protección de los activos de Información de la empresa y de sus clientes es vital para el correcto alineamiento con los objetivos de negocio. Con este fin, se ha establecido un Sistema de Gestión de Seguridad de la Información (SGSI) que implementa todos los procesos y controles necesarios para establecer la forma en que se protegen los activos de Información.

El Sistema de Gestión de Seguridad de la Información se actualiza y mejora continuamente para satisfacer las necesidades del negocio, de los clientes y de las partes interesadas, se establecen nuevos objetivos de forma periódica y se evalúan regularmente los procesos de negocio.

6. Aprobación y revisión

El Sistema de Gestión de Seguridad de la Información se revisa anualmente o cuando se produce un cambio significativo en el negocio.

El Sistema de Gestión de Seguridad de la Información implementado, operado y mejorado, en base al Esquema Nacional de Seguridad (CCN) en la organización garantiza:

- Que establece y mantiene el contexto, determina las necesidades y expectativas de las partes interesadas
- Que los roles, responsabilidades y autoridades están asignados
- Que se establecen objetivos para el Sistema de Gestión de Seguridad de la Información, alineados con los objetivos estratégicos
- Que se establecen indicadores para medir el rendimiento de los controles y, se analizan y evalúan periódicamente
- Que se establece un criterio de riesgo para la identificación, el análisis, la evaluación y el tratamiento de riesgos
- Que todo el personal recibe formación y concienciación respecto a la Seguridad de la Información y las políticas de Seguridad de la Información (control de acceso físico y lógico, seguridad física, Ante código malicioso, copias de seguridad, clasificación de la información, tratamiento de la información, continuidad…) implementadas en la empresa
- Que el Sistema de Gestión se opera en base a la información documentada aprobada, políticas, procesos, procedimientos, …
- Que se verifica el cumplimiento a través de auditorías externas, seguimientos de los objetivos e indicadores y de las revisiones por la dirección.

- Que se corrigen las no conformidades y quejas, mediante la implementación de acciones correctivas, y la evaluación del resultado de las mismas.
- Que se realiza la mejora continua sobre el Sistema de Gestión de Seguridad de la Información.

Los principios de la Política de Seguridad de la Información son asumidos e impulsados por la Dirección, quien proporciona los medios necesarios y dota a los empleados de los recursos suficientes para su cumplimiento, plasmándolos y poniéndolos en público conocimiento a través de una Política estratégica de Seguridad.

00-2 Política de la Seguridad de la Información

7. Desarrollo de la política de seguridad de la información

Esta política de seguridad de la información complementa las políticas de seguridad de la empresa en diferentes materias de seguridad disponibles en la intranet.

Esta política se desarrollará por medio de políticas 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 comunicación.

La empresa trata datos de carácter personal. Los accesos a determinados documentos de seguridad sólo tendrán acceso las personas autorizadas y los responsables correspondientes. Todos los sistemas de información de la empresa 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 mencionado documento de seguridad.

La normativa de seguridad estará disponible en la intranet.

Esta política se desarrolla aplicando los principios básicos siguientes:

a) Profesionalidad
   La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado.

   Todo el personal debe disponer de formación específica sobre seguridad de la información

   Los proveedores serán evaluados y deberían disponer de personal con la formación adecuada a los servicios que realicen.

b) Mejora continua del sistema de gestión de la seguridad

La gestión del sistema de gestión se basa en la mejora continua, actualizándolo y revisándolo periódicamente.

c) Declaración de aplicabilidad
Se dispone del documento 610-1 donde se establecen todas las medidas de seguridad referidas en el Esquema Nacional de Seguridad, RD 3/2020 anexo II, con referencia a las política y registros establecidos dentro del sistema de gestión de la seguridad y como mínimo con referencia a:

Marco Organitzativo	-
Marco Operacional	Planificación
Marco Operacional	Control de acceso
Marco Operacional	Explotación
Marco Operacional	Servicios externos
Marco Operacional	Continuidad del servicio
Marco Operacional	Monitorización del sistema
Medidas de protección	Protección de infraestructuras
Medidas de protección	Gestión del personal
Medidas de protección	Protección de equipos
Medidas de protección	Protección de las comunicaciones
Medidas de protección	Protección de los servicios

La declaración de aplicabilidad siguiente sólo es copia, siendo el único documento actualizado el que está registrado como registro 610-1 en el sistema de gestión integrado.

ENS (RD 3/2010)												Aplicabilidad
	Dimensiones					B	M	A				
Apartado RD 3/2010									Marco	Apartado	Descripción de la medida	(Si/No)
Art. 29	D	I	C	A	T	Aplica			General	-	INSTRUCCIONES TÉCNICAS DE SEGURIDAD Y GUÍAS DE SEGURIDAD	SI
Art. 35	D	I	C	A	T	Aplica			General	-	INFORME DEL ESTADO DE LA SEGURIDAD	SI

INTERFACE SAFEACCESS	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

FECHA:	25/05/2022	**EDICIÓN:**	**2**

ENS (RD 3/2010)												Aplicabilidad
	Dimensiones					B	M	A				
Art. 36	D	I	C	A	T	Aplica			General	-	CAPACIDAD DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	SI
Art. 43, 44	D	I	C	A	T	Aplica			General	-	CATEGORIAS Y FACULTADES	SI
Org. 1	D	I	C	A	T	Aplica			Marco Organitzativo	-	Política de seguridad	SI
Org. 2	D	I	C	A	T	Aplica			Marco Organitzativo	-	Normativa de seguridad	SI
Org. 3	D	I	C	A	T	Aplica			Marco Organitzativo	-	Procedimientos de Seguridad	SI
Org. 4	D	I	C	A	T	Aplica			Marco Organitzativo	-	Proceso de autorización	SI
Op. Pl.1	D	I	C	A	T	Aplica	Aplica	**No aplicado**	Marco Operacional	Planificación	Análisis de riesgos	SI
Op. Pl.2	D	I	C	A	T	Aplica	Aplica	**No aplicado**	Marco Operacional	Planificación	Arquitectura de seguridad	SI

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

FECHA:	25/05/2022	EDICIÓN:	2

ENS (RD 3/2010)												Aplicabilidad
	Dimensiones					B	M	A				
Op. Pl.3	D	I	C	A	T	Aplica			Marco Operacional	Planificación	Adquisición de nuevos componentes	SI
Op. Pl.4	D						Aplica		Marco Operacional	Planificación	Dimensionamiento / Gestión de la Capacidad	SI
Op. Pl.5	D	I	C	A	T			No aplicado	Marco Operacional	Planificación	Componentes certificados	NO
Op.acc.1				A	T	Aplica			Marco Operacional	Control de acceso	Identificación	SI
Op.acc.2		I	C	A	T	Aplica			Marco Operacional	Control de acceso	Requisitos de acceso	SI
Op.acc.3		I	C	A	T		Aplica		Marco Operacional	Control de acceso	Segregación de funciones y tareas	SI
Op.acc.4		I	C	A	T	Aplica			Marco Operacional	Control de acceso	Proceso de gestión de derechos de acceso	SI
Op.acc.5		I	C	A	T	Aplica	Aplica	No aplicado	Marco Operacional	Control de acceso	Mecanismos de autenticación	SI
Op.acc.6		I	C	A	T	Aplica	Aplica	No aplicado	Marco Operacional	Control de acceso	Acceso local (*local logon*)	SI
Op.acc.7		I	C	A	T	Aplica			Marco Operacional	Control de acceso	Acceso remoto (*remote login*)	SI
Op.exp.1	D	I	C	A	T	Aplica			Marco Operacional	Explotación	Inventario de activos	SI

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

FECHA:	25/05/2022	EDICIÓN:	2

ENS (RD 3/2010)												Aplicabilidad
	Dimensiones					B	M	A				
Op.exp.2	D	I	C	A	T	Aplica			Marco Operacional	Explotación	Configuración de seguridad (bastionado)	SI
Op.exp.1	D	I	C	A	T		Aplica		Marco Operacional	Explotación	Gestión de la configuración	SI
Op.exp.4	D	I	C	A	T	Aplica			Marco Operacional	Explotación	Mantenimiento	SI
Op.exp.5	D	I	C	A	T		Aplica		Marco Operacional	Explotación	Gestión de Cambios	SI
Op.exp.6	D	I	C	A	T	Aplica			Marco Operacional	Explotación	Protección frente al código dañino	SI
Op.exp.7	D	I	C	A	T		Aplica		Marco Operacional	Explotación	Gestión de Incidentes	SI
Op.exp.8					T	Aplica	Aplica	No aplicado	Marco Operacional	Explotación	Registro de la Actividad de los Usuarios	SI
Op.exp.9					T		Aplica		Marco Operacional	Explotación	Registro de la gestión de incidentes	SI
Op.exp.10					T			No aplicado	Marco Operacional	Explotación	Protección de los registros de actividad	NO
Op.exp.11	D	I	C	A	T	Aplica	Aplica		Marco Operacional	Explotación	Protección de las claves criptográficas	SI
Op.ext.1	D	I	C	A	T		Aplica		Marco Operacional	Servicios externos	Contratación y acuerdos de nivel de servicio	SI
Op.ext.2	D	I	C	A	T		Aplica		Marco Operacional	Servicios externos	Gestión diaria	SI
Op.ext.3	D							No aplicado	Marco Operacional	Servicios externos	Medios alternativos	NO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

FECHA:	25/05/2022	EDICIÓN:	2

ENS (RD 3/2010)												Aplicabilidad
	Dimensiones					B	M	A				
Op.cont.1	D						Aplica		Marco Operacional	Continuidad del servicio	Análisis de impacto (BIA)	SI
Op.cont.2	D							No aplicado	Marco Operacional	Continuidad del servicio	Plan de continuidad	NO
Op.cont.3	D							No aplicado	Marco Operacional	Continuidad del servicio	Pruebas periódicas	NO
Op.mom.1	D	I	C	A	T		Aplica		Marco Operacional	Monitorización del sistema	Detección de intrusión	SI
Op.mom.2	D	I	C	A	T	Aplica	Aplica	No aplicado	Marco Operacional	Monitorización del sistema	Sistema de métricas	SI
Mp.if.1	D	I	C	A	T	Aplica			Medidas de protección	Protección de infraestructuras	Áreas separadas y con control de acceso	SI
Mp.if.2	D	I	C	A	T	Aplica			Medidas de protección	Protección de infraestructuras	Identificación de las personas	SI
Mp.if.3	D	I	C	A	T	Aplica			Medidas de protección	Protección de infraestructuras	Acondicionamiento de los locales	SI
Mp.if.4	D					Aplica			Medidas de protección	Protección de infraestructuras	Energía eléctrica	SI
Mp.if.5	D					Aplica	Aplica		Medidas de protección	Protección de infraestructuras	Protección frente a incendios	SI

INTERFACE SAFEACCESS	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

FECHA:	25/05/2022	**EDICIÓN:**	**2**

ENS (RD 3/2010)											Aplicabilidad
	Dimensiones					B	M	A				
5.1.6	D						Aplica		Medidas de protección	Protección de infraestructuras	Protección frente a inundaciones	SI
5.1.7	D	I	C	A	T	Aplica			Medidas de protección	Protección de infraestructuras	Registro de entrada y salida de equipamiento	SI
5.1.8	D							**No aplicado**	Medidas de protección	Protección de infraestructuras	Instalaciones alternativas	**NO**
Mp.per.1	D	I	C	A	T		Aplica		Medidas de protección	Gestión del personal	Caracterización del puesto de trabajo	SI
Mp.per.2	D	I	C	A	T	Aplica			Medidas de protección	Gestión del personal	Deberes y obligaciones	SI
Mp.per.3	D	I	C	A	T	Aplica			Medidas de protección	Gestión del personal	Concienciación	SI
Mp.per.4	D	I	C	A	T	Aplica			Medidas de protección	Gestión del personal	Formación	SI
Mp.per.5	D							**No aplicado**	Medidas de protección	Gestión del personal	Personal alternativo	**NO**

INTERFACE SAFEACCESS	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

FECHA:	25/05/2022	**EDICIÓN:**	**2**

ENS (RD 3/2010)												Aplicabilidad
	Dimensiones					B	M	A				
Mp.eq.1	D	I	C	A	T	Aplica	Aplica		Medidas de protección	Protección de equipos	Puesto de trabajo despejado	SI
Mp.eq.2				A			Aplica	No aplicado	Medidas de protección	Protección de equipos	Bloqueo del puesto de trabajo	SI
Mp.eq.3	D	I	C	A	T	Aplica		No aplicado	Medidas de protección	Protección de equipos	Protección de los equipos portátiles	SI
Mp.eq.4	D						Aplica		Medidas de protección	Protección de equipos	Medios alternativos	SI
Mp.com.1	D	I	C	A	T	Aplica		No aplicado	Medidas de protección	Protección de las comunicaciones	Perímetro seguro	SI
Mp.com.2			C				Aplica	No aplicado	Medidas de protección	Protección de las comunicaciones	Protección de la confidencialidad	SI
Mp.com.3		I		A		Aplica	Aplica	No aplicado	Medidas de protección	Protección de las comunicaciones	Protección de la autenticidad e integridad	SI
Mp.com.4	D	I	C	A	T			No aplicado	Medidas de protección	Protección de las comunicaciones	Segregación de redes	NO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

FECHA:	25/05/2022	EDICIÓN:	2

ENS (RD 3/2010)											Aplicabilidad
	Dimensiones					B	M	A				
Mp.com.5	D							No aplicado	Medidas de protección	Protección de las comunicaciones	Medios alternativos	NO
Mp.si.1			C			Aplica			Medidas de protección	Protección de los soportes información	Etiquetado	SI
Mp.si.2		I	C				Aplica	No aplicado	Medidas de protección	Protección de los soportes información	Criptografía	SI
Mp.si.3	D	I	C	A	T	Aplica			Medidas de protección	Protección de los soportes información	Custodia	SI
Mp.si.4	D	I	C	A	T	Aplica			Medidas de protección	Protección de los soportes información	Transporte	SI
Mp.si.5			C			Aplica	Aplica		Medidas de protección	Protección de los soportes información	Borardo y destrucción	SI
Mp.s.1	D	I	C	A	T	Aplica			Medidas de protección	Protección de los servicios	Protección del correo electrónico	SI
Mp.s.2	D	I	C	A	T	Aplica		No aplicado	Medidas de protección	Protección de los servicios	Protección de servicios y aplicaciones web	SI
Mp.s.3	D						Aplica	No aplicado	Medidas de protección	Protección de los servicios	Protección frente a denegación de servicio	SI
Mp.s.4	D							No aplicado	Medidas de protección	Protección de los servicios	Medios alternativos	NO

8. Nivel requerimiento

El nivel de seguridad requerido es **MEDIO**, dentro del marco establecido en el artículo 43 y los criterios generales prescritos en el Anexo I del ENS. Algunos de los criterios que determinan dicho nivel es que el proceso está totalmente definido. El catálogo de procesos se mantiene actualizado y garantizan la consistencia de las actuaciones entre las diferentes partes de la organización.

Además de haber normativa establecida y procedimientos para poder reaccionar ante cualquier incidente de seguridad y se actualiza y mantiene de forma regular. Así mismo, existe una alta coordinación entre departamentos y los proyectos llevados a cabos.

El comité STIC contempla la posibilidad de modificar el nivel de seguridad requerido.

Los principios de la Política de Seguridad de la Información son asumidos e impulsados por la Dirección, quien proporciona los medios necesarios y dota a los empleados de los recursos suficientes para su cumplimiento, plasmándolos y poniéndolos en público conocimiento a través de la presente Política de Seguridad.

9. Aprobación política

Jordi Mateu
Dirección
INTERFACE SAFEACCESS, S.L.

A fecha 25 de mayo del 2022