

| | | | |
|---------------|------------|-----------------|---|
| FECHA: | 02/06/2022 | EDICIÓN: | 1 |
|---------------|------------|-----------------|---|

Índice

| | | |
|----|---|---|
| 1. | Marco normativo..... | 1 |
| 2. | Responsabilidades y organización de la seguridad..... | 1 |
| a. | Comité STIC (Seguridad TIC)..... | 1 |
| b. | Funciones y responsabilidades..... | 2 |
| 3. | Designación y renovación de los roles de seguridad..... | 4 |
| 4. | Gestión del riesgo..... | 4 |
| 5. | Recursos..... | 4 |
| 6. | Aprobación y revisión..... | 5 |
| 7. | Desarrollo de la política de seguridad de la información..... | 6 |
| 8. | Nivel requerimiento..... | 6 |
| 9. | Aprobación política..... | 7 |

FECHA: 02/06/2022 **EDICIÓN:** 1

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. |

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 | Sebastià Prat |
| Responsable de la información | Leopold Pons |
| Responsable del servicio | Josep Prat |
| Responsable de la Seguridad | Leopold Pons |
| | |
| | |

| | | | |
|---------------|------------|-----------------|---|
| FECHA: | 02/06/2022 | EDICIÓN: | 1 |
|---------------|------------|-----------------|---|

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 | Leopond Pons | Responsable de la implementación, configuración y mantenimiento de los servicios de seguridad relacionados con las TIC |
| Operadores sistemas TIC | Flexible IT, S.L. | Equipo de continuidad. Son los responsables de la operación diaria de los servicios de seguridad relacionados con las TIC |
| | | |
| | | |

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.

| | | | |
|---------------|------------|-----------------|---|
| FECHA: | 02/06/2022 | EDICIÓN: | 1 |
|---------------|------------|-----------------|---|

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

FECHA: 02/06/2022 **EDICIÓN:** 1



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

| | | | |
|---------------|------------|-----------------|---|
| FECHA: | 02/06/2022 | EDICIÓN: | 1 |
|---------------|------------|-----------------|---|

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.

| | | | |
|---------------|------------|-----------------|---|
| FECHA: | 02/06/2022 | EDICIÓN: | 1 |
|---------------|------------|-----------------|---|

- 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.

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.

| | | | |
|---------------|------------|-----------------|---|
| FECHA: | 02/06/2022 | EDICIÓN: | 1 |
|---------------|------------|-----------------|---|

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

| |
|--|
|  flexible  NIF: B-63002927 C/ Vallhonrat, 45 - 08221 Terrassa www.flexible.com Josep Prat Dirección |
|--|

A fecha 02 de junio de 2022.