StockCrowd	POLÍTICA DE SEGURIDAD

FECHA:	30/11/2025	EDICIÓN:	2

Índice

StockCrowd	POLÍTICA DE SEGURIDAD

FECHA:	30/11/2025	EDICIÓN:	2

1. Aprobación y entrada en vigor

Texto aprobado el día 30 de Noviembre de 2025 por la dirección de StockCrowd, de ahora en adelante la empresa.

Esta Política de Seguridad de la Información está vigente desde la fecha de aprobación (o publicación para las entidades que sea obligatoria su publicación oficial) y hasta que sea reemplazada por una nueva Política.

2. Objetivos de la organización

La empresa se apoya en sus sistemas de información para alcanzar sus objetivos estratégicos. Por ello, la gestión diligente y la protección de estos sistemas son prioritarias. Debemos aplicar medidas adecuadas, basadas en una evaluación de riesgos, para salvaguardarlos de cualquier incidente, intencionado o accidental, que pueda comprometer la autenticidad, trazabilidad, integridad o confidencialidad de la información, o la disponibilidad de los servicios.

La seguridad de la información tiene como meta primordial garantizar la operatividad continua de la empresa, permitiéndole cumplir con sus funciones y ofrecer servicios de alta calidad. Para lograrlo, es fundamental adoptar un enfoque preventivo, supervisar activamente las operaciones diarias y responder con agilidad a cualquier incidente.

Los sistemas TIC están expuestos a un panorama de amenazas dinámico que podría impactar negativamente la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad uso previsto y valor de la información y los servicios. Para defendernos eficazmente, se requiere una estrategia de seguridad adaptable que se ajuste a los cambios del entorno. Esto implica que cada departamento debe implementar las medidas de seguridad obligatorias del Esquema Nacional de Seguridad (ENS), realizar un seguimiento constante de los niveles de prestación de servicios, analizar las vulnerabilidades detectadas y contar con planes de respuesta a incidentes para asegurar la continuidad del negocio.

Es imperativo que la seguridad TIC sea un pilar fundamental en cada etapa del ciclo de vida de un sistema: desde su concepción y desarrollo hasta su adquisición, operación y eventual retirada. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incorporados en la planificación, así como en las solicitudes de ofertas y los pliegos de licitación para proyectos que gestionen datos personales, involucren la compra de servicios TIC o afecten a nuestros sistemas de información.

3. Alcance

Esta política se aplica a todos los sistemas de información de la empresa a las personas que conforman la organización y a los prestadores de servicios o proveedores de soluciones TIC de la empresa.

4. Misión

StockCrowd desarrolla y comercializa software para captar donaciones on-line a través de un modelo SaaS (en la nube) B2B.

Los objetivos en materia de seguridad que la empresa pretende garantizar con la presente Política serán:

- Garantizar la confidencialidad, integridad, autenticidad y trazabilidad de la información y la continuidad en la prestación de los servicios.
- Implementar medidas de seguridad en función del riesgo.
- Formar y concienciar a los integrantes de la empresa respecto a la seguridad de la información. Implementar medidas de seguridad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones.
- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.
- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, logrando que la información que sea transmita a través de redes de comunicaciones sea adecuadamente protegida.
- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

- Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema.
- Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a reproducirse.
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.
- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

5. Principios rectores de la política

✔ Alcance estratégico: la seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de la empresas y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente

✔ Seguridad integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de la información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.

✔ Gestión de la seguridad basada en el riesgo: la gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a que esté sujeta la información y sus sistemas. y serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.

✔ Prevención, detección, respuesta y conservación con la implementación de acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y, cuando estas se produzcan, danto una respuesta ágil para restaurar la información o servicios prestados, garantizando una conservación segura de la información.

- ✔ Existencia de líneas de defensa, la estrategia de seguridad de la empresa se diseña e implementa en capas de seguridad.
- ✔ Vigilancia continua y reevaluación periódica: la empresa implementa medios la detección y respuesta a actividades o comportamientos anómalos. Además, de otros que permitan una evaluación continuada del estado de seguridad de los activos, Existirá, también, un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.
- ✔ Seguridad por defecto y desde el diseño: los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.
- ✔ Diferenciación de responsabilidades, en aplicación de este principio las funciones del Responsable de la Seguridad y del Responsable del Sistema estarán diferenciadas.

6. Alcance de certificación

Los Sistemas de Información que dan soporte al desarrollo y comercialización del software en la nube "Stockcrowd" para la captación de donaciones on-line.

7. 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 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
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

Nº	Legislación
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	DIRECTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión

8. 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 (*)	
Responsable del servicio (*)	
Responsable de la Seguridad (**)	
Responsable de la Sistema (**)	

(*) Estas funciones pueden recaer en la misma persona
(**) Estas funciones **no** pueden recaer en la misma persona

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

StockCrowd	POLÍTICA DE SEGURIDAD

FECHA:	30/11/2025	**EDICIÓN:**	**2**

Administrador sistemas TIC		Responsable de la implementación, configuración y mantenimiento de los servicios de seguridad relacionados con las TIC
Operadores sistemas TIC		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 implementados y mantenidos.
- 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 con los objetivos.

Las funciones del Responsable de Seguridad de la Información son:

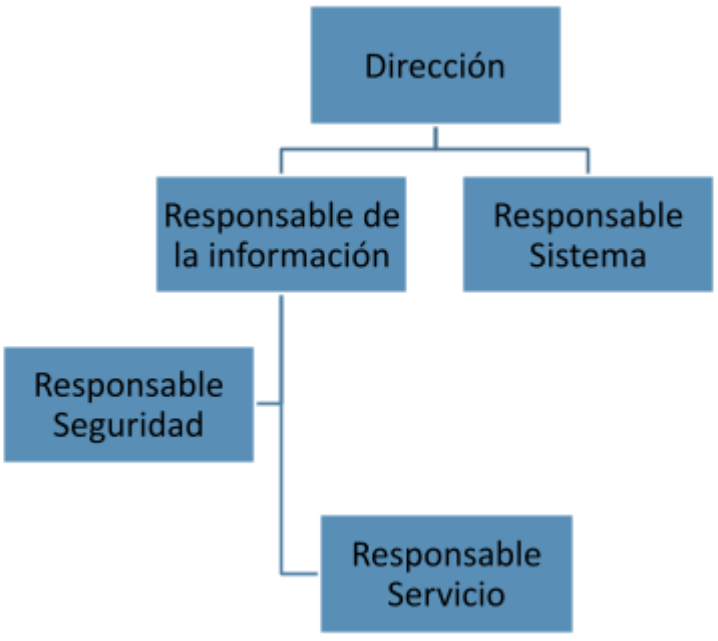
- Coordinar y controlar las medidas de seguridad de la información y de protección de datos.

- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:
  - La estrategia de seguridad de la información será 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.

Responsable del Sistema

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.

Dependencias de los roles



9. 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 archivado por el Responsable de Seguridad.
El organigrama establecido refleja 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.

10. Resolución de conflictos

En el caso de conflictos entre los diferentes responsables, el Comité de Seguridad de la Información podrá dirimir las discrepancias

11. Gestión del riesgo

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 se produzcan cambios en la información manejada.
- cuando se produzcan cambios en los servicios prestados.
- cuando ocurra un incidente grave de seguridad.
- cuando se reporten vulnerabilidades graves.
- cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o en las evaluaciones de impacto.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Se tendrán en cuenta los riesgos en protección de datos, contando con la opinión del Delegado de Protección de Datos, en caso de que hubiere, además se coordinarán los planes del tratamiento del riesgo.

12. 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.

13. Datos de carácter personal

La empresa trata datos de carácter personal, según se describe en el Registro de Actividades del Tratamiento. La empresa deberá evaluar los riesgos relacionados con los datos personales tratados proponiendo un plan de actuación para la corrección de aquellos riesgos que superen el umbral autorizado.

El análisis de riesgos será reevaluado de forma periódica, contando con el asesoramiento y supervisión que realice el Delegado de Protección de Datos, y, en todo caso, cuando se detecte un tratamiento de alto riesgo, debiendo realizar, en su caso, una evaluación de impacto. La implementación del plan de tratamiento del riesgo se coordinará con el del ENS, así como el resto de los procedimientos o normas de seguridad con las derivadas de las obligaciones en materia de protección de datos, especialmente en el control de los prestadores de servicios o la respuesta a incidentes y/o brechas de datos personales.

14. Desarrollo de la política de seguridad de la información

Esta Política se desarrollará por medio de normativa de seguridad que aborde aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la empresa que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible por diversos medios a disposición de los usuarios en la intranet de la empresa, en la carpeta compartida con otra información de relevancia para los empleados en materia de protección para ciber-riesgos.

Disponer de formación específica sobre seguridad de la información.

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

15. Obligaciones del personal

Todos los miembros de la empresa tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y las normas, procedimientos o guías que la desarrollen, siendo responsabilidad de la empresa a través del Comité de Seguridad y del área de personal de disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de la empresa atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la empresa, 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.

16. Terceras partes / prestadores de servicios / proveedores de soluciones

Cuando la empresa preste servicios a otras entidades o maneje información de otras, se les hará partícipes de esta Política de Seguridad de la Información, sin perjuicio de respetar las obligaciones de la normativa de protección de datos si actúa como encargado del tratamiento en la prestación de los citados servicios, y se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y procedimientos de actuación para la reacción ante incidentes de seguridad. Además, el Responsable de Seguridad (o persona en quien delegue) será el Punto de Contacto (POC).

StockCrowd	POLÍTICA DE SEGURIDAD

FECHA:	30/11/2025	**EDICIÓN:**	**2**

Cuando la empresa 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 atañe a dichos servicios o información, sin perjuicio del cumplimiento de otras obligaciones en materia de protección de datos. En la contratación de prestadores de servicios o adquisición de productos se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS.

En la adquisición de derechos de uso de activos en la nube tendrá en cuenta los requisitos establecidos en las medidas de seguridad del Anexo II y las Guía de desarrollo.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, de modo que la empresa pueda supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte. Se establecerán procedimientos específicos de reporte y resolución de incidencias que deberán ser canalizadas por el POC de los terceros implicados y, además, cuando se afecte a datos personales por el Delegado de Protección de Datos. Los terceros garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

Cuando algún aspecto de la Política no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, el Responsable de la Seguridad emitirá un informe 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 del inicio de la contratación o, en su caso, de la adjudicación. El informe se trasladará al representante de la empresa que deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo los riesgos detectados.

Cuando la empresa adquiera, desarrolle o implante un sistema de Inteligencia Artificial, además de cumplir con lo establecido en la normativa vigente en la materia, deberá contar con el informe del Responsable de la Seguridad, que consultará al Responsable de la Información y del Servicio y, cuando sea necesario, al del Sistema, debiendo también el Delegado de Protección de Datos emitir su parecer.

17. Gestión de incidentes de seguridad

La empresa dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios.
Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como la de protección de datos personales u otra que afecte al organismo para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y, cuando sea preciso, a las Fuerzas y Cuerpos de Seguridad el Estado o los juzgados.

18. Categoría de seguridad

La categoría de seguridad requerida es **MEDIA**, dentro del marco establecido en el artículo 40 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.

19. Aprobación de la política y entrada en vigor

Las modificaciones de la presente Política que supongan cambios o adaptaciones ante ineficiencias las realizará el Comité de Seguridad de la Información, que deberá revisar anualmente.

En caso de que los cambios supongan una modificación sustancial o de los principios o responsabilidades designadas, el Comité de Seguridad propondrá los cambios que deberán ser aprobados, en su caso, por la persona u órgano con las debidas competencias.

StockCrowd	POLÍTICA DE SEGURIDAD

FECHA:	30/11/2025	**EDICIÓN:**	**2**

La sustitución de la Política será instada por el Comité de Seguridad de la Información y ratificada por la persona u órgano con las debidas competencias, de lo que se informará adecuadamente a los interesados por los mismos canales usados para su difusión.

Fecha: 30/11/2025

Aprobado por:
CEO