

Política de Seguridad

Noviembre 2022

Propietario

Antonio Fernández Ruiz
Director de Tecnología



Índice

1	INTRODUCCIÓN	3
2	OBJETO	3
3	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	3
4	ALCANCE.....	4
4.1	EMPLEADOS	4
4.2	SISTEMAS DE INFORMACIÓN	4
4.3	TERCERAS PARTES.....	5
5	ROLES Y RESPONSABILIDADES.....	5
5.1	USUARIOS	5
5.2	PROPIETARIOS.....	5
5.3	ADMINISTRADORES.....	5
6	MANTENIMIENTO, APROBACIÓN Y REVISIÓN DE LA POLÍTICA	6
7	DISTRIBUCIÓN DE LA POLÍTICA.....	6
8	SANCIONES	7

1 Introducción

Los procesos de negocio de Fullstep dependen en gran medida de los Sistemas de Información y la Información que almacenan. La presente Política tiene como misión establecer las directrices globales de Seguridad para la organización, así como proteger los activos de información.

Estas directrices incluyen la adopción de una serie de medidas organizativas y normas que se presentan en este documento y se desarrollan en sus documentos asociados y cuya finalidad es la de proteger los recursos de información de Fullstep y los sistemas de información utilizados para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y legalidad de la información.

Esta Política está basada en las recomendaciones de buenas prácticas para garantizar la Seguridad en la Gestión de Sistemas de Información (Normas internacionales ISO 27001 e ISO 27002), así como en la legislación vigente aplicable a la materia.

2 Objeto

El objetivo principal de la creación de esta Política es garantizar a los usuarios el acceso a la información con la cantidad y calidad que se requiera para el desempeño, así como evitar serias pérdidas de información y accesos no autorizados a la misma.

3 Política de seguridad de la información

Como respuesta a un nuevo entorno tecnológico donde la convergencia entre la informática y las comunicaciones están facilitando un nuevo paradigma de productividad para las empresas, Fullstep está altamente comprometida ofreciendo sus servicios de Consultoría, servicios de soporte a la función de compras y desarrollo e implantación de sistemas de gestión de compras en un entorno de calidad, donde el uso de buenas prácticas en seguridad es fundamental para conseguir los objetivos de confidencialidad, integridad, disponibilidad y legalidad de toda la información gestionada para el progreso de Fullstep.

En consecuencia, Fullstep define las siguientes directrices de aplicación a tener en cuenta:

- **Confidencialidad:** La información tratada por Fullstep será conocida exclusivamente por las personas autorizadas, previa identificación, en el momento y por los medios habilitados.

- **Integridad:** La información tratada por Fullstep será completa, exacta y válida, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación.
- **Disponibilidad:** La información tratada por Fullstep estará accesible y utilizable por los usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad prevista.
- **Legalidad:** Fullstep garantizará el cumplimiento de toda legislación que le sea de aplicación. Y en concreto, la normativa en vigor relacionada con el tratamiento de datos de carácter personal.

Mediante esta Política, la Dirección General asume la responsabilidad de apoyar y promover el establecimiento de las medidas organizativas, técnicas y de control necesarias para el cumplimiento de las directrices de seguridad aquí descritas. En este sentido, esta Política de Seguridad será mantenida, actualizada y adecuada a los fines de la organización, alineándose con el contexto de gestión de riesgos de la organización. A este efecto, se revisará a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia. Los cambios y modificaciones serán aprobados e impulsados por la Dirección General de Fullstep.

4 Alcance

4.1 Empleados

La Seguridad de la Información es un esfuerzo conjunto. Requiere la implicación y participación de todos los miembros de la organización que trabajan con Sistemas de Información. Por ello, cada empleado debe cumplir los requerimientos de la Política de Seguridad y su documentación asociada. Los Empleados que deliberadamente o por negligencia incumplan la Política de Seguridad serán sometidos a las acciones disciplinarias según se contempla en el último capítulo de este documento.

4.2 Sistemas de información

Esta Política afecta a todos los activos de información de la Compañía, tanto a la información en soporte manual o papel, de carácter personal o no y albergada en equipos personales o servidores, redes, aplicaciones, sistemas operativos, procesos de la empresa que pertenecen y/o son administrados por Fullstep. Esta Política cubre los aspectos más directamente relacionados con la responsabilidad y buen uso del personal.

4.3 Terceras partes

La presente Política de Seguridad es de extensible conocimiento y cumplimiento para cualquier persona externa perteneciente a terceras entidades que realice cualquier tipo de tratamiento sobre la información propiedad de Fullstep. Asimismo, esta Política y sus procedimientos asociados serán de obligado cumplimiento para las empresas terceras proveedoras contratadas para la ejecución de servicios profesionales en los ámbitos que se consideren oportunos, en el caso de que realicen cualquier actividad que implique acceso o tratamiento a cualquier sistema o información propiedad de Fullstep y así se definirá contractualmente.

5 Roles y Responsabilidades

5.1 Usuarios

Los usuarios deben conocer y aplicar las Políticas de Seguridad, procedimientos, estándares y aplicar la legislación vigente. Deben entenderlos y cumplir con los mismos.

En general, cualquier persona que genera información es responsable de su clasificación de acuerdo con las instrucciones de la Compañía. Asimismo, cualquier persona que utiliza información y los sistemas de información está obligada a gestionarlos con el cuidado necesario, así como de utilizarlos únicamente para realizar las tareas autorizadas y en cumplimiento de la normativa. Esto también es aplicable al personal externo.

5.2 Propietarios

Los propietarios de activos de información generalmente se corresponden con la Dirección General, o responsables de Área, quienes deben adquirir, desarrollar y mantener aplicativos de la Compañía como sistemas de soporte a las decisiones y otras actividades de la misma.

Los propietarios deben indicar la clasificación de sus activos que mejor corresponde con su valor crítico, disponibilidad e importancia relativa para la organización. Su clasificación marcará el nivel de riesgo y de protección, así como el nivel de acceso a dicha información o aplicativo.

5.3 Administradores

Los administradores son Empleados a cargo de salvaguardar la información de la Compañía propia y cedida por terceros.

Cada sistema de información debe disponer de, al menos, un Administrador autorizado según consta en el Documento de Seguridad.

Son los responsables de almacenar la información, implementar controles de acceso (para prevenir accesos no autorizados) y ejecutar copias de seguridad periódicas (para asegurar la disponibilidad de la información crítica).

6 Mantenimiento, aprobación y revisión de la Política

El Responsable de Seguridad de la Información es el responsable de establecer y mantener la Política de Seguridad, manuales y procedimientos correspondientes de Fullstep.

La Dirección General de la Compañía es la responsable de la aprobación y publicación de la Política, de distribuirla a todos los Empleados y terceros afectados, así como revisar y evaluar la Política de Seguridad.

Cualquier cambio o evolución que afecte o pudiera afectar al contenido de esta Política de Seguridad quedará registrado en una nueva firma del documento de aprobación. De esta forma se concreta y confirma el compromiso por la seguridad de la información.

Periódicamente, y en todo caso no superando el plazo de un año, se revisará la vigencia y razonabilidad de la presente Política y se llevarán a cabo las mejoras, adaptaciones o modificaciones requeridas en función de los cambios organizativos, técnicos o regulatorios aplicables.

7 Distribución de la Política

El documento de Política de Seguridad será accesible a todo el personal interno, se entregará en la incorporación de un nuevo empleado y cada 12 meses se distribuirá por correo electrónico y en la Herramienta corporativa "<https://wiki.fullstep.net/>" a todos los Empleados internos y externos subcontratados por Fullstep que manejen datos y recursos pertenecientes a la misma para conocimiento y conciencia de las normas de seguridad dispuestas.

Asimismo, se obtendrá compromiso de la lectura y aceptación de la misma por parte de todos los Empleados.

Cualquier cambio sustancial en el documento será distribuido a todos los usuarios a través de una notificación formal, enviada por correo electrónico o por comunicación interna en medios accesibles a los mismos mediante un modelo de comunicación habilitada para tal efecto.

8 Sanciones

Cualquier violación premeditada o negligente de las políticas y normas de seguridad y que suponga un potencial daño, consumado o no a Fullstep, será sancionada de acuerdo a los mecanismos habilitados en el convenio de la Compañía y en la normativa legal, contractual y corporativa vigentes.

Todas las acciones en las que se comprometa la seguridad de Fullstep y que no estén previstas en esta Política, deberán ser revisadas por la Dirección General y por el Responsable de Seguridad para dictar una resolución sujetándose al criterio de la Compañía y la legislación prevista.

Las acciones disciplinarias en respuesta a los incumplimientos de la Política de Seguridad son atribución de los Responsables de Departamento en conjunción con Administración y la Dirección General.

En Madrid, a 3 de noviembre de 2022

Antonio Fernández Ruiz

Director de Tecnología