



*POLÍTICA DE
SEGURIDAD DE LA
INFORMACIÓN*

DISCOVER CYBERSEC TRANSFORM OPTIMIZE INNOVATE EMPOWER

myCloudDoor.com



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Version 1.0.
12 / 02 / 2024

FICHA DEL DOCUMENTO

Nombre del Fichero	Política de Seguridad de la información
Tipología	Política
Ámbito de Difusión	Todos los empleados y colaboradores exxternos de myCloudDoor
Responsable	Responsable del Sistema de Gestión Integrado
Nivel de sensibilidad	Interno

CONTROL DE VERSIONES

Version	Realiza	Revisa	Aprueba	Fecha	Descripción
1.0	Comité Operativo del Sistema de Gestión	Comité Estratégico del Sistema de Gestión	Jorge Flores Catalina Jiménez	12/02/2024	Versión inicial del documento



CONTENIDO

INTRODUCCIÓN	3
ALCANCE	3
OBJETIVOS	3
PRINCIPIOS	4
MARCO NORMATIVO	5
ORGANIZACIÓN DE LA SEGURIDAD	6
GESTIÓN DE RIESGOS	6
OBLIGACIONES DEL PERSONAL	6
TERCERAS PARTES	7
APROBACIÓN	7

1 | INTRODUCCIÓN

En un entorno cada vez más interconectado y digitalizado, donde la información se ha convertido en uno de los activos más valiosos para nuestra organización, la importancia y dependencia de los sistemas TIC (Tecnologías de Información y Comunicaciones) es cada vez mayor. Por este motivo, es cada vez más necesario garantizar que estos sistemas sean administrados con la debida diligencia, adoptando una estrategia de seguridad alineada con la cultura y los requisitos de negocio, que nos permita disponer de la capacidad necesaria para detectar, reaccionar y recuperarnos eficazmente frente a aquellas amenazas que puedan afectar a la disponibilidad, integridad o confidencialidad, así como a la autenticidad y trazabilidad de la información tratada y los servicios que prestamos.

Es por ello que, en myCloudDoor Solutions, S.L. y myCloudDoor Security & Innovation S.L. (en adelante myCloudDoor), consideramos la seguridad de la información como uno de los ejes principales en el desarrollo de nuestras actividades y, en consecuencia, ponemos a disposición los recursos y medios necesarios para implementar las medidas de seguridad en el cumplimiento de los requisitos aplicables y la gestión de los riesgos a los que se expone la organización.

2 | ALCANCE

La presente política aplica a todos los sistemas TIC de la organización y a todo el personal, tanto interno como externo colaborador con la organización, que dan soporte tanto al tratamiento de la información de la cual somos responsables y a la prestación de los servicios que ofrecemos.

3 | OBJETIVOS

Nuestra misión es aportar las soluciones que mejor que se adaptan a las necesidades de nuestros clientes, integrando las tecnologías de la información, la gestión industrial y la gestión empresarial. Para ello, pretendemos ser un referente tecnológico, que genere confianza a largo plazo, liderado por personas comprometidas y orgullosas de pertenecer a myCloudDoor.

Con este fin, y conscientes de la necesidad de ofrecer garantías para una protección efectiva de los recursos corporativos y la continuidad y correcto funcionamiento de nuestros servicios, hemos determinado los siguientes objetivos:

- Establecer y mantener un Sistema de Gestión de la Seguridad de la Información eficiente y eficaz, alineado con la legislación vigente y estándares internacionales en materia de seguridad.

- Minimizar los riesgos a los que la organización y los activos de información están expuestos, de los cuales es responsable, hasta niveles de riesgo aceptable.
- Cumplir, y hacer cumplir, en las relaciones con terceros, con los requisitos y obligaciones de seguridad conforme al marco legal, normativo y contractual establecido.

Promover la seguridad mediante procesos de formación y concienciación, garantizando que los empleados de la organización disponen de las competencias necesarias.

Garantizar la protección de la información y la continuidad de los procesos críticos de la organización en la prestación de servicios a nuestros clientes.

Asimismo, para lograr alcanzar estos objetivos, establecemos planes de actuación y seguimiento que se evalúan periódicamente.

4 | PRINCIPIOS

El desarrollo normativo de la presente política, así como la toma de decisiones dentro del sistema de gestión, se basan en el siguiente conjunto de principios básicos:

- La seguridad como un proceso integral, constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información.
- Gestión de la seguridad basada en los riesgos, permitiendo así el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables mediante una apropiada aplicación de medidas de seguridad.
- Prevención, detección, respuesta y conservación, al objeto de minimizar las vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.
- Líneas de defensa, constituidas por medidas organizativas, físicas y lógicas, como estrategia de protección por capas.
- Vigilancia continuada para la detección de actividades o comportamientos anómalos y su oportuna respuesta.
- Reevaluación periódica del estado de la seguridad de los activos, midiendo la evolución de los riesgos, detectando vulnerabilidades e identificando deficiencias y oportunidades de mejora.
- La seguridad como función diferenciada, separando las responsabilidades de definición de requisitos, supervisión de la seguridad y la explotación de los sistemas.

5 | MARCO NORMATIVO

En myCloudDoor cumplimos con todos los requisitos legales, regulatorios y contractuales que nos son de aplicación, tanto en materia de seguridad de la información como en privacidad. De igual forma, nos comprometemos al cumplimiento de las medidas determinadas en aquellos marcos de referencia y estándares internacionales que implantamos, destacando, entre otros, las siguientes referencias certificables:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, para sistemas de información de nivel ALTO.
- ISO/IEC 27001:2022 Sistemas de gestión de seguridad de la información.
- ISO/IEC 27701:2019 Sistemas de Gestión de Privacidad de la Información.

Para ello, en myCloudDoor desarrollamos la presente política mediante un conjunto de procesos documentados que conforman nuestro cuerpo normativo del sistema de gestión.

Esta normativa está a disposición de todo el personal de myCloudDoor y terceras partes interesadas que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información.

6 | ORGANIZACIÓN DE LA SEGURIDAD

Con el fin de facilitar la gestión y el mantenimiento del Sistema de Gestión, en myCloudDoor hemos determinado una estructura definida, aprobada y funcional de roles y responsabilidades para la implementación, operación y gestión de la seguridad de la información y la privacidad dentro de la organización, atendiendo al principio de seguridad como función diferenciada.

Adicionalmente, la atención, supervisión y auditoría de la seguridad de los sistemas, a lo largo de todo el ciclo de vida, es realizada por personal debidamente cualificado y capacitado para ello.

7 | GESTIÓN DE RIESGOS

La gestión de riesgos en myCloudDoor es un proceso fundamental que se realiza sobre todos nuestros sistemas de información, a través del cual identificamos, evaluamos y controlamos los riesgos que pueden afectar al desempeño en la prestación de nuestros servicios, la protección de la información, incluidos los que pudieran afectar a los datos de carácter personal, o la capacidad para alcanzar nuestros objetivos.

Este proceso se ejecuta de forma recurrente y continua, manteniéndose actualizado en todo momento, a fin de adaptarnos a los nuevos retos y amenazas con motivo de los cambios constantes sobre nuestro entorno.

No obstante, con carácter de mínimos, esta evaluación se repite:

- Regularmente, al menos una vez al año.
- Cuando exista un cambio significativo en los sistemas de información.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Asimismo, con el fin de obtener resultados objetivos, comparables y reproducibles, alineados con los requerimientos para la prestación de nuestros servicios, myCloudDoor dispone y aplica una metodología de análisis y gestión de riesgos reconocida, documentada y formalmente aprobada.

8 | OBLIGACIONES DEL PERSONAL

Todo el personal de myCloudDoor tiene la obligación de conocer y cumplir con esta Política de Seguridad de la Información y con el cuerpo normativo de seguridad, según sea de aplicación, que desarrolla las medidas y protocolos a cumplir para la protección de la información.

De igual forma, el personal tiene la obligación de formarse en aquellas funciones relacionadas con el desempeño de sus competencias con profesionalidad y ética, especialmente en lo que se refiere al uso, operación o administración de los sistemas TIC, y de atender a las sesiones o actividades de concienciación en materia de seguridad de la información y privacidad.

La Dirección de myCloudDoor pone a disposición del personal los medios y recursos necesarios para que las iniciativas de formación y concienciación puedan realizarse de forma efectiva. En este sentido, myCloudDoor dispone de un plan de formación y concienciación continua, que es revisado periódicamente, para atender las necesidades de todos los empleados según sus funciones y responsabilidades.

9 | TERCERAS PARTES

En aquellos casos en los que myCloudDoor presta servicios o maneja información de terceros, se les hace partícipes de esta Política de Seguridad de la Información y normativa en la medida que se requiera.

Para poder reaccionar de forma rápida y eficaz ante incidentes de seguridad que pueda

afectar a servicios de terceros, establecemos canales de reporte y coordinación, y protocolos de actuación.

En myCloudDoor no cedemos información a terceros, salvo previa autorización de los interesados, y que estos terceros ofrezcan garantías suficientes del cumplimiento de las medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos establecidos en su Política de Seguridad de la Información, y previa autorización de los interesados.

En aquellos casos en los que se utilicen servicios de terceros o se ceda información a terceros, bajo las condiciones antes mencionadas, transmitimos también los requisitos de seguridad aplicables y perseguimos su cumplimiento. Asimismo, cuando interviene personal de terceros en la operación o administración de nuestros sistemas, nos aseguramos de que están adecuadamente capacitados y concienciados en materia de seguridad. Se adoptarán las medidas oportunas en caso de incumplimiento de estos requerimientos por parte de un tercero.

10 | APROBACIÓN

La presente política ha sido aprobada por la Dirección de myCloudDoor Solutions, S.L. y myCloudDoor Security & Innovation S.L., siendo efectiva desde la fecha de su aprobación y hasta que la misma sea reemplazada por la aprobación de una nueva versión de la misma.

Asimismo, de acuerdo con el proceso de mejora continua, esta política es revisada regularmente por la Dirección, a fin de contrastar la oportunidad, idoneidad, completitud y precisión de su contenido, con el objetivo de que se adapte a las circunstancias de nuestro entorno.

Mediante esta política, la Dirección de myCloudDoor quiere dejar constancia del compromiso con el cumplimiento de los requisitos aplicables en materia de seguridad de la información y la mejora continua de los procesos, que conforman el sistema de gestión, y que desarrollan las directrices para la gestión y protección de la información que trata myCloudDoor y los servicios que presta.



myCloudDoor.com

GRACIAS

info@myclouddoor.com