

DOCUMENTO 2.
POLÍTICA DE
SEGURIDAD DE LA
INFORMACIÓN

five
flames
mobile



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN FIVE FLAMES MOBILE

El presente documento pretende recoger las directrices que debe seguir el Sistema de Gestión de la Seguridad de la Información de acuerdo con las necesidades de FIVE FLAMES MOBILE y a la legislación vigente. Además, se definen las pautas de actuación en caso de incidentes y se definen las responsabilidades.

Control de versiones

Responsable del documento	vortega
----------------------------------	---------

Versión	Observaciones	Autor	Fecha
1.0	Creación del documento	vortega	10/02/2019
2.0	Revisión de contenidos	vortega	31/03/2020
3.0	Revisión del contenido después de la auditoría externa	vortega	12/08/2020
4.0	Revisión de contenido	vortega	10/07/2022

1	<u>DEFINICIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y OBJETIVOS</u>	4
2	<u>DECLARACIÓN POR PARTE DE LA DIRECCIÓN APOYANDO LOS OBJETIVOS Y PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN</u>	6

1 Definición de la seguridad de la información y objetivos

La Política de Seguridad de la Información es la declaración general que representa la posición de la dirección de FIVE FLAMES MOBILE con respecto a la protección de los activos de información (datos personales, información sobre el proceso de Desarrollo y tecnologías de información incluido el hardware y el software), a la implementación del Sistema de Gestión de Seguridad de la Información y al apoyo, generación y publicación de sus políticas, procedimientos e instrucciones.

Esta Política de Seguridad aplica a toda la empresa FIVE FLAMES MOBILE, su dirección, sus empleados, sus clientes, sus socios y se implementará en el PROCESO DE DESARROLLO DE APLICACIONES MÓVILES.

FIVE FLAMES MOBILE, para el cumplimiento de su misión, visión, objetivo estratégico y apegado a sus valores corporativos, establece la función de Seguridad de la Información en la entidad, con el objetivo de:

1. Generales

- Minimizar el riesgo en las funciones más importantes de la entidad principalmente relacionadas con el proceso de Desarrollo.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de sus clientes, socios y empleados.
- Implementar el Sistema de Gestión de Seguridad de la Información.
- Garantizar la respuesta efectiva de la empresa ante incidentes de seguridad.

2. Protección de Activos de información:

- Se debe garantizar que solo los usuarios autorizados puedan acceder a objetos de información en el sistema.
- La capacidad de asegurar todos los tipos de recursos del sistema es una fortaleza del sistema.
- Se deben definir cuidadosamente las diferentes categorías de usuarios que pueden acceder al sistema.
- Se deben definir qué tipos de autorizaciones de acceso se otorgarán a los distintos grupos de usuarios.

3. Autenticación

- Se deben verificar que los accesos de cualquier tipo son realizados por quien realmente dice ser, evitándose la suplantación de identidad.
- Se deben utilizar contraseñas lo suficientemente fuertes para controlar el acceso de los usuarios o incluso la utilización de certificados digitales como método de autenticación para el acceso de los diversos activos de la empresa.
- Se debe controlar que los usuarios autenticados tengan los permisos correctos en base a su rol y nivel de autorización.

4. Autorización

- Definir los diferentes niveles de autorización discriminando que usuarios tienen autorización para el acceso a determinados recursos.
 - Establecer los mecanismos para revocar las autorizaciones periódicamente y garantizar que las personas que acceden a determinadas informaciones son las que se han determinado.
5. Integridad de la Información
- Hay que asegurar que la información se mantenga íntegra dentro de las operaciones que se realizan:
 - Integridad de datos: proteger la información contra modificaciones o manipulaciones no autorizadas estableciendo medidas contra los riesgos de que alguien acceda y modifique la información de forma no autorizada.
 - Integridad del sistema: protección de los sistemas para que siempre proporcionen resultados consistentes.
 - Confidencialidad: la información sensible se debe mantener en entornos privados y protegidos utilizándose medidas especiales orientadas al cifrado de datos y conexiones seguras.
6. Auditoría de actividades de seguridad
- Vigilancia y registro de posibles incidentes para prevenir eventos no deseados.

2 Declaración por parte de la Dirección apoyando los objetivos y principios de la seguridad de la información

FIVE FLAMES MOBILE ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, alineado a las necesidades de la empresa y a los requerimientos obligatorios.

FIVE FLAMES MOBILE protegerá la información generada, procesada o resguardada por los procesos de la empresa, su infraestructura tecnológica y activos del riesgo que se puede generar por el uso interno de datos o por el acceso otorgado a terceras personas (p.ej.: clientes o proveedores)

FIVE FLAMES MOBILE protegerá la información creada, procesada, transmitida o resguardada por sus procesos empresariales, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad.

FIVE FLAMES MOBILE protegerá su información de las amenazas originadas por parte del personal de la empresa.

FIVE FLAMES MOBILE protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

FIVE FLAMES MOBILE controlará la operación de sus procesos empresariales, garantizando la seguridad de los recursos tecnológicos y las redes de datos.

FIVE FLAMES MOBILE implementará control de acceso a la información, sistemas y recursos de red.

FIVE FLAMES MOBILE garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

FIVE FLAMES MOBILE garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

FIVE FLAMES MOBILE garantizará la disponibilidad de sus procesos empresariales y la continuidad de su operación basada en el impacto que pueden generar los eventos imprevistos.

FIVE FLAMES MOBILE garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.