POLÍTICA DE SGSI, SEGURIDAD Y ENS - FCC INDUSTRIAL

Política de Gestión de la Seguridad de la Información del sistema de Seguridad y del Esquema Nacional de Seguridad

FCC Industrial utiliza y trata en su actividad diaria una gran cantidad de información para poder cumplir con sus objetivos de negocio. La Dirección de FCC Industrial, consciente de la necesidad de promover, mantener y mejorar el enfoque hacia el cliente en todas sus actividades, ha implantado un Sistema de Gestión Integrado (SGSI, Seguridad y ENS) conforme a estándares cuyo objetivo final es asegurar que entendemos y compartimos las necesidades y metas de nuestros clientes, intentando prestar servicios que cumplan sus expectativas trabajando en la mejora continua. La presente Política de Gestión de Seguridad de la Información, del sistema de Seguridad y del Esquema Nacional de Seguridad, integrada en este documento, y la normativa relacionada con ella, establecen un marco de trabajo que permite que la información se gestione de forma segura, real y eficaz y de acuerdo al propósito de la organización. Con este objeto se busca **la implicación de todo el personal de la organización** en la aplicación de las medidas que se determinen. Por ello, uno de los objetivos primordiales de esta política es dar a conocer, tanto las directrices adoptadas como los objetivos que buscan cubrir con todo ello, dado el papel activo que en su consecución desempeñarán todas las personas de la empresa.

FCC Industrial manifiesta expresamente su compromiso de potenciar la Seguridad y Ciberseguridad de la Información del servicio prestado, y se compromete a satisfacer las necesidades y expectativas de las partes interesadas, y a mantener alta nuestra competitividad en los servicios y productos detallados en el **alcance**, según el **marco legal** y regulatorio en el que se desarrollan las actividades, y que se especifican en el MCMA_ Manual Sistema Gestión Calidad de FCC Industrial.

FCC Industrial es consciente, tanto de la importancia de la seguridad de la información que trata y de la importancia de asegurar la **confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad** de sus sistemas de **información**, como del carácter irreemplazable e inherente al trabajo en el día a día y parte esencial del servicio que se presta a nuestros clientes, dentro de unos parámetros que aseguren la calidad y eficacia del servicio de tecnología de la información:

- La gestión de la seguridad deberá ser conforme con los **requisitos** del sistema de gestión de seguridad de la información y del ENS y deberá adecuarse a lo establecido en la normativa legal vigente.
- La información es un recurso estratégico para FCC Industrial y, por tanto, se debe garantizar su adecuada **protección** en el desempeño de la actividad diaria y en las relaciones con entidades externas.
- La seguridad y ciberseguridad de la información son tareas que implican a todo el personal de FCC Industrial, tanto de forma individual como a través de la cooperación entre los distintos departamentos, servicios y unidades. Es preciso contar con **personal sensible** a las necesidades de un buen sistema de seguridad de la información.
- Difundir y que sea asumida, la **normativa** de seguridad en la información, del sistema de seguridad y del ENS, de obligado cumplimiento, entre todo el personal de FCC Industrial, en los distintos niveles.
- Determinar y considerar los **riesgos y oportunidades** con el fin de asegurar que el sistema de gestión de seguridad de la información pueda conseguir los resultados previstos, prevenir o reducir efectos indeseados y lograr la mejora continua. Identificar los riesgos y adoptar medidas de protección frente a las **amenazas** contra la seguridad de la información proporcionales al valor de los activos a proteger, los riesgos existentes y el impacto de los posibles fallos de seguridad,

incluidos los riesgos que se derivan del tratamiento de los datos personales (según Normativa interna del Grupo FCC en materia de LOPD).

- Preservar la **confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad** de la información durante su tratamiento, independientemente del medio en el que esté contenida, y del lugar donde se encuentre.
- Compromiso de **mejora continua** del proceso de seguridad y del sistema de gestión de seguridad de la información, y de que sea reexaminada esta política en las reuniones de Dirección con este objeto.
- FCC Industrial se adhiere a las **políticas** de seguridad de la información del Grupo FCC.

MISIÓN y OBJETIVOS:

FCC Industrial define, además, estos **objetivos generales** para la aplicación de estas políticas:

- Establecer una estrategia de análisis y gestión de riesgos orientados a la mejor comprensión de estos y de sus salvaguardas.
- Establecer las necesidades básicas de protección, los planes de seguridad para aplicar las salvaguardas.
- Organizar la seguridad en base a criterios de clasificación de la información, responsabilidad de los propietarios de esta, descripciones de tareas y procedimientos, procedimientos ante violaciones de la seguridad, consecuencias disciplinarias ante incumplimiento de las normas de seguridad, verificaciones de conformidades en Seguridad y gestión de la configuración y de los cambios.
- Fomentar la mejora continua de los servicios y soporte al cliente.
- Continuar el posicionamiento de FCC Industrial como referente en el sector.
- Proporcionar soluciones para transformar los datos y la información para ayudar en la toma de decisiones de nuestros clientes.
- Proporcionar a los clientes el equipo más profesional y disponer de forma inmediata y durante el tiempo necesario de técnicos altamente cualificados, expertos en las disciplinas requeridas y acostumbrados a trabajar en equipo.
- Tener una prestación del servicio basada en nuestro compromiso con la mejora continua de nuestros sistemas, con la seguridad y ciberseguridad de la información como pilar central y por defecto.

El objetivo último de la seguridad de la información es asegurar que una organización pueda cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes **Principios Básicos**:

Política de Gestión de la Seguridad de la Información del sistema de Seguridad y del Esquema Nacional de Seguridad

a. Seguridad como proceso integral.

b. Gestión de la seguridad basada en los riesgos.

c. Prevención, detección, respuesta y conservación.

d. Existencia de líneas de defensa.

e. Vigilancia continua

f. Reevaluación periódica.

g. Diferenciación de responsabilidades.

Nuestra **misión** y objetivos los conseguiremos a través del cumplimiento de los siguientes **Requisitos Mínimos:**

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de la actividad y detección de código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

- Un sistema de **objetivos**, métricas e indicadores de mejora continua, seguimiento, medición de nuestros procesos internos, así como de la satisfacción de nuestros clientes. Estableciendo y

supervisando el cumplimiento de los requisitos contractuales para asegurar un servicio eficaz y seguro.

- Formando y concienciando continuamente a nuestro equipo para tener el mayor grado de **profesionalidad** y especialización posible, además teniendo nuestras infraestructuras en un estado adecuado y en concordancia con los requerimientos de nuestros clientes.
- Con un procedimiento seguro de gestión de adquisición de productos.
- Cumpliendo las exigencias de la legislación vigente, especialmente con el Reglamento General de Protección de Datos y el cumplimiento de nuestra **Documentación de Seguridad**. Las directrices para la estructuración de la **documentación de seguridad del sistema**, su gestión y acceso está detallada en el PR_FCCIND_120_01 Gestión y Seguridad de la información.
- Introduciendo los procesos de mejora continua que permitan un avance permanente en nuestra gestión de Seguridad de la Información.
- Gestionando y elaborando planes para la gestión y tratamiento de los riesgos con una metodología de análisis y gestión de riesgos utilizada, basada en estándares.
- Gestionando las comunicaciones internas y externas e información almacenada y en tránsito.
- Asegurando la interconexión con otros sistemas de información.
- Gestionando y monitorizando la actividad con la gestión de logs.
- Con especial atención a la gestión de **incidentes de seguridad.**
- Asegurando la **continuidad** y disponibilidad del negocio y de los servicios.
- Asegurar que nuestros Activos y Servicios cumplen con las medidas del ENS del nivel establecido para las dimensiones de **Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad.**

Estos principios se deberán contemplar en las siguientes áreas de seguridad:

- **Física:** Comprendiendo la seguridad de las dependencias, instalaciones, sistemas hardware, soportes y cualquier activo de naturaleza física que trate o pueda tratar información, así como los accesos físicos.
- **Lógica:** Incluyendo los aspectos de protección de aplicaciones, redes, comunicación electrónica, sistemas informáticos y con los accesos lógicos.
- **Político-corporativa:** Formada por los aspectos de seguridad relativos a la propia organización, a las normas internas, regulaciones y normativa legal.

POLÍTICA DE SGSI, SEGURIDAD Y ENS - FCC INDUSTRIAL

Política de Gestión de la Seguridad de la Información del sistema de Seguridad y del Esquema Nacional de Seguridad

Roles o funciones de seguridad:

En FCC contamos con responsables de la información, de sistemas, de seguridad de la información y del servicio, cuyas funciones y responsabilidades han sido aceptadas por los responsables respectivos.

El Comité de Seguridad de la Información de FCC Industrial es el mecanismo de coordinación y resolución de conflictos

Las funciones de los responsables y del propio Comité se reflejan en el Procedimiento PR_FCCIND_120_01 Gestión y Seguridad de la información.

Todas las normas que se dicten en aras de lograr estos objetivos vincularán a las personas responsables de su aplicación, y en general a toda la organización en su cumplimiento.

Aprobado por

Miguel Ángel Mayor Gamo

Director General FCC Industrial I. E.