POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Dirección de **CENTRIBAL** 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 (SGI) conforme al estándar 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. 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, a mantener alta nuestra competitividad en los servicios de DIGITALCARE.
Esta política de seguridad de la información establece el marco normativo bajo el cual Centribal garantiza la seguridad, confidencialidad, integridad, disponibilidad. Esta política aplica a todos los empleados, colaboradores y terceros con acceso a los sistemas de información de Centribal.

MISIÓN y OBJETIVOS*:*

- Fomentar la mejora continua de los servicios al cliente.
- Continuar el posicionamiento de **CENTRIBAL** como referente en el sector.
- Implantar, mantener y comprobar nuestros mecanismos de continuidad de la actividad para garantizar que la información y los servicios vitales estén a disposición de nuestros clientes cuando sea necesario.
- 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.
- Implantar una cultura de seguridad de la información mediante la formación y la sensibilización.
- Garantizar que nuestros sistemas y redes de información se mantienen y protegen eficazmente frente a amenazas internas y *externas*

Nuestra **misión** y objetivos lo conseguiremos a través de:

- 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 **GDPR** y el cumplimiento de nuestros procedimientos de seguridad.
- 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.
- 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.

Así mismo, 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.

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:

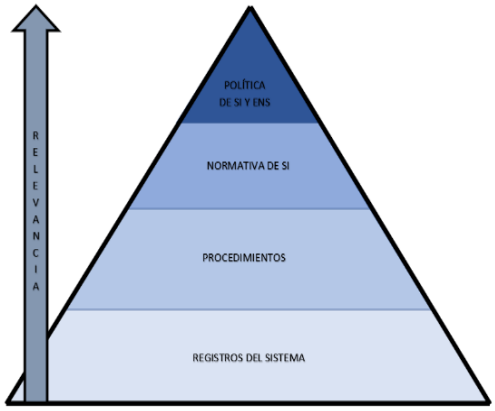
a) Seguridad integral.
b) Gestión de riesgos.
c) Prevención, reacción y recuperación.
d) Líneas de defensa.
e) Reevaluación periódica.
f) Función diferenciada.

- Mantenimiento y aplicación del Documento de Aplicabilidad del SGI

Componen el CSI:

- Responsable de la Información
- Responsable del Servicio
- Responsable de Seguridad de la información
- Responsable del Sistema

Estructuración de la documentación de seguridad del sistema
La documentación del sistema sigue la siguiente estructura:



La clasificación de la información del sistema se clasifica en las siguientes categorías, tal y como se establece en documento Normativa de Seguridad

- Uso Publico
- Uso Interno
- Uso Confidencial

Legislación aplicable en materia de tratamiento de datos de carácter personal
En materia de tratamiento de datos de carácter personal se tendrá en cuenta, principalmente, el 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 y la legislación nacional correspondiente.
El marco legal y regulatorio aplicable se encuentran recogido en el documento Registro Identificación y evaluación de requisitos legales.
Los riesgos que se derivan del tratamiento de los datos personales se analizan en el documento Gestión de Riesgos de Privacidad de LOPD

Considerando estas pautas, esta dirección reitera su más firme compromiso aunando esfuerzos para el logro de estos objetivos, por lo que esta política es entendida, implantada y tenida al día en todos los niveles de la organización.

Fdo.

Dirección