



EXTRACTO

POLÍTICA DE SEGURIDAD
DE LA INFORMACIÓN
GRUPO BANCA MARCH

ÍNDICE

1. INTRODUCCIÓN Y OBJETIVOS
2. ALCANCE
3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN



1. INTRODUCCIÓN

La seguridad de la información es un ámbito por tratar para la gestión de riesgos empresariales. La carencia o falta de protección de la información en el Grupo Banca March podría repercutir de manera significativa en impactos de distinta índole (financiero, regulatorio, reputacional, etc.).

La Política de Seguridad de la Información del Grupo Banca March tiene como propósito establecer una estrategia basada en el modelo de mejora continua para la prevención, detección y reacción ante cualquiera de las amenazas que afecten a la seguridad de la información en el desarrollo de sus servicios y actividades, así como reducir el riesgo introducido por el uso de las tecnologías de información en los procesos y servicios del Grupo Banca March. El enfoque de la seguridad de la información se mantendrá alineado en todo momento con los objetivos estratégicos del Grupo.

2. ÁMBITO DE APLICACIÓN

Esta Política se aplica en todo el Grupo Banca March, por lo que los principios establecidos en ella afectan a toda la información en soporte electrónico o soporte papel y a los sistemas de información propiedad del Grupo Banca March o gestionados para el mismo. Todas las entidades del Grupo están alineadas a los principios y objetivos que se exponen en esta Política.

El Grupo Banca March se compromete a que todo el personal, tanto interno como externo, esté familiarizado con la Política, ya que su cumplimiento es necesario para la protección de los activos de información del Grupo.

3. PRINCIPIOS BÁSICOS Y OBJETIVOS ESTRATÉGICOS DE LA SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información del Grupo Banca March establece los objetivos y los principios básicos de seguridad de la información, que todo el personal, tanto interno como externo, de todas las unidades del Grupo, así como proveedores de servicios deben satisfacer.

El Grupo Banca March considera que la consecución de los objetivos de la Entidad se encuentra sujeta al cumplimiento de diversos requerimientos que tienen como objetivo garantizar la seguridad de la información dentro de la organización.

Por tanto, la seguridad de la información debe ser una prioridad para el Grupo y para ello, la presente Política establece los siguientes principios básicos:

1. **Confidencialidad**

Garantizar que la información solo esté disponible para aquellos que tienen autorización para acceder a ella. La confidencialidad de la Información debe garantizarse en todo momento para asegurar la protección de la misma frente al uso no autorizado, revelaciones accidentales, violación de la privacidad y otras acciones similares de accesos de terceros no permitidos. La información de la que el Grupo Banca March es propietario y/o depositario debe ser únicamente accesible para las personas debidamente autorizadas, pertenezcan o no al Grupo.

2. **Integridad**

Mantener la exactitud y completitud de la información y prevenir su alteración no autorizada. La integridad de la información debe asegurarse a través de todos los procesos (con dependencia de la tecnología y las personas tanto automáticos como manuales) que la gestionan, procesan y almacenan para asegurar que se cubre toda la información necesaria y suficiente para la marcha de los servicios y procesos en cada uno de los sistemas informáticos y procesos transaccionales.

3. **Disponibilidad**

Asegurar que la información esté disponible y accesible cuando sea necesario. La disponibilidad de la Información y la capacidad de su procesamiento manual y automático debe garantizarse mediante las adecuadas medidas de respaldo y continuidad del negocio cuando sea necesario, de manera tal que no se interrumpa significativamente la marcha de los servicios.

4. **Autenticidad**

Verificar la autenticidad de los usuarios y la validez de la información. La autenticidad de la información debe ser, estableciendo los procedimientos y controles necesarios, garantizar que la información es auténtica, completa, exacta, sin alteraciones o manipulaciones.

5. **Trazabilidad**

Garantizar la implementación de un conjunto de medidas, acciones y procedimientos que permitan registrar e identificar qué eventos se han producido sobre los sistemas de información y quiénes son los usuarios responsables que los han generado.

Para la consecución de los propósitos de esta Política, el Grupo establece una estrategia preventiva de análisis que persigue los siguientes objetivos:

1. **Priorización de la seguridad de la información**

La Política establece que la seguridad de la información es fundamental para el logro de los objetivos de la Entidad, elevándola a un nivel estratégico y asegurando la involucración de los órganos de dirección del Grupo.

2. **Enfoque holístico de la seguridad de la información**

La Política abarca los cinco pilares fundamentales de la seguridad de la información: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Esto garantiza una protección integral de la información.

3. **Aplicación a todos los niveles**

La Política se aplica a todo el personal, interno y externo, así como a los proveedores de servicios, asegurando que la seguridad de la información sea una responsabilidad compartida en todo el Grupo.

4. **Gestión proactiva del riesgo**

La Política establece un enfoque preventivo para la gestión de riesgos, que incluye la identificación, mitigación y reevaluación continua de los riesgos que podrían afectar la seguridad de la información.

5. **Alineación con el apetito de riesgo**

La Política garantiza un nivel de riesgo aceptable dentro de los umbrales de tolerancia, asegurando que la gestión de riesgos esté alineada con el marco de apetito al riesgo aprobado.

6. **Mejora continua**

La Política establece un ciclo de mejora continua para la gestión de riesgos, asegurando que el Grupo se adapte a las cambiantes amenazas y vulnerabilidades.



Palma de Mallorca
Av. Alexandre Rosselló, 8
07002 Palma de Mallorca

971 779 111
bancamarch.es