Política de Seguridad de la Información

Índice

1 Política de Seguridad de la Información

1.1 Objetivos

El objetivo principal de la presente Política de Seguridad de la Información de Colonial es la definición de las medidas organizativas, técnicas, físicas y legales, necesarias para proteger los activos de información (entendidos como datos de los Sistemas de información de necesarios para el buen funcionamiento de la compañía o especialmente sensibles que requieran de ser protegidos) de la Organización[1] contra actuaciones no autorizadas (entendidas como accesos, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso), que se puedan producir de forma intencional o accidental.

1.2 Alcance

La presente Política es aplicable a todos los empleados del grupo Colonial, así como colaboradores, contratistas y proveedores externos que tengan acceso a los activos de la información propiedad de la Organización.

1.3 Cumplimiento

El cumplimiento de la Política de Seguridad de la Información es obligatorio. Si los empleados, colaboradores, contratistas o proveedores externos violan esta Política, la Organización se reserva el derecho de tomar las medidas correspondientes.

1.4 Aprobación y Revisiones

La aprobación de la Política de Seguridad de la Información así como de sus modificaciones corresponde al Consejero Delegado y a la Dirección General Corporativa *(en adelante la Dirección)*. La Política deberá ser revisada, como mínimo, una vez al año o cuando se produzcan cambios significativos en los sistemas de información.

[1] *Las referencias a la Organización engloban a todas las sociedades del Grupo Colonial domiciliadas y gestionadas en España.*

2 Descripción de la Política

2.1 Introducción

De conformidad con el Código Ético de Colonial (apartado 6.6) la información es un activo que la compañía considera esencial para las actividades de la empresa y debe ser protegida de acuerdo con los principios de confidencialidad, integridad y disponibilidad.

A través de esta Política se difunden los objetivos de seguridad de la información de la Compañía, que se consiguen a través de la aplicación de controles de seguridad, para gestionar un nivel de riesgo aceptable. Este documento tiene el objetivo de garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos de negocio y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad en Colonial.

2.2 Organización de Seguridad

La Dirección de TI es responsable de definir, coordinar y controlar la gestión necesaria para mitigar los riesgos asociados a la seguridad de la información en Colonial.

Las medidas de seguridad se estructurarán en un Cuerpo Normativo de Seguridad *(en adelante CNS)*, a tres niveles de la siguiente forma:

- *"Política de Seguridad de la Información"* que manifiesta los principios básicos de seguridad de la información, que han de guiar el desarrollo del CNS.
- *"Políticas"*, que detallan a alto nivel el objetivo de cada área en las cuales se divide el CNS.
- *"Procedimientos"*, que establecen los pasos concretos a seguir para implementar los controles definidos por las Políticas.

2.3 Responsabilidad

Todos los empleados deben conocer, comprender y cumplir el CNS de Colonial. Este CNS aplica a todas las sociedades del grupo Colonial domiciliadas y gestionadas desde España. Será responsabilidad entonces de todos los empleados y colaboradores proteger los activos de la información. En caso de incumplimiento de dicho CNS, Colonial podrá ejercer las acciones disciplinarias establecidas en su código ético, así como las acciones legales que correspondan.

2.4 Seguridad de la información

El término "Seguridad de la Información" se refiere a la protección de los activos de información contra la revelación, modificación o destrucción no autorizada, ya sea ocasionada de forma accidental o intencionada. Los atributos de seguridad asociados a los activos de información son:

- **Confidencialidad**: Propiedad por la que la información se pone a disposición o se revela únicamente a individuos, entidades o procesos autorizados.

- **Integridad**: Propiedad de salvaguardar la exactitud y completitud de los activos de información.

- **Disponibilidad**: Propiedad de ser accesible y utilizable por una entidad autorizada en el momento requerido.

2.5 Alcance

El alcance de este CNS incluye los activos de información en soporte electrónico.

2.6 Directrices de la Política

La Dirección de Colonial considera que la consecución de los objetivos del grupo se encuentra sujeta al cumplimiento de diversos requerimientos encaminados a garantizar la Seguridad de la Información dentro de la Organización. De esta manera, se considera que la Seguridad de la Información debe ser una prioridad y para ello, la presente Política establece las siguientes directrices:

- El acceso a los recursos de información estará basado en el principio de mínimo privilegio, lo cual será llevado a cabo mediante una correcta definición de roles y perfiles, garantizando una adecuada segregación de funciones, tanto en los sistemas como en la gestión de la seguridad.

- La presente Política, deberá ser accesible para todos los miembros de Colonial, así como a los profesionales y colaboradores externos que se relaciona con la Organización a través de alguno de sus procesos.

- La Organización deberá cumplir con todos aquellos requerimientos legales, regulatorios y estatuarios que le sean de aplicación, así como los requerimientos contractuales.

- La confidencialidad de la información deberá garantizarse en todo momento.

- La integridad de la información deberá asegurarse a través de todos los procesos que la gestionan, procesan y almacenan.

- La disponibilidad de la información deberá garantizarse mediante las adecuadas medidas de respaldo y continuidad de negocio.

- Colonial garantizará que todo el personal dentro del alcance de la Política dispondrá de la adecuada formación y concienciación en materia de Seguridad de la Información.

- Todo incidente o debilidad que pueda comprometer o haya comprometido la confidencialidad, integridad y/o disponibilidad de la información, deberá ser registrado y analizado para aplicar las correspondientes medidas correctivas y/o preventivas.

2.7 Comité de Seguridad de la Información

Se constituye un Comité de Seguridad compuesto, al menos, por:

- La Dirección General Corporativa
- La Dirección de TI, como responsable máximo de seguridad de los sistemas de información.
- El auditor interno.

El Comité se reunirá periódicamente para tratar cualquier incidente en seguridad o cambios en la política o procedimientos.

El Comité, para un mejor cumplimiento de sus funciones, podrá invitar a sus sesiones a cualquier miembro del equipo directivo, del personal o cualquier profesional externo que considere necesario.

Las resoluciones y los acuerdos del Comité serán adoptados por mayoría simple.

2.8 Funciones y Responsabilidades de la Dirección de TI

La Dirección de TI, además de las responsabilidades propias de su posición no especificadas en este documento, como responsable de la función de Seguridad TI, deberá cumplir con las siguientes responsabilidades:

- Conocer y aprobar en los casos que sea requerido, todas las compras, adquisiciones o contrataciones de activos TI.
- Implementar, mantener y mejorar el CNS, así como supervisar el cumplimiento del mismo.
- Coordinar las revisiones del CNS (periódicas y ad hoc) con los responsables implicados y formalizar los resultados de estos.
- Supervisar la recolección, documentación y actualización de los indicadores clave de seguridad, así como su reporting al Comité de Seguridad.
- Supervisar los incidentes de seguridad, acciones correctivas y preventivas.
- Gestionar las herramientas y plataformas de seguridad de Colonial.

2.9 Cumplimiento Legal

La presente Política establece la necesidad de cumplir con todos los requerimientos legislativos, normativos y contractuales que le sean de aplicación a Colonial y los activos de información gestionados.

Toda solución de servicios o infraestructura tecnológica debe garantizar que su selección está de acuerdo con las condiciones contractuales, de legislación y regulación externa e interna, para el debido cumplimiento de los regímenes legales a los cuales está sometida la Organización.

2.9.1 Protección de Datos

Los estándares de seguridad son de obligatorio cumplimiento para los empleados y los colaboradores con acceso a los datos de carácter personal y a los sistemas de información.

Los requisitos definidos por la normativa vigente aplicable relacionados con el tratamiento de datos de carácter personal tienen que ser difundidos y entendidos por el personal.

2.10 Compromiso de la Dirección

El compromiso de la Dirección de Colonial con lo establecido en la Política de Seguridad de la Información para apoyar el cumplimiento de los objetivos del negocio es firme, este compromiso se refleja en la aprobación, definición de modelo de gobierno, difusión y revisión de la propia Política.

Las Políticas de Seguridad de la Información serán aprobadas por la Dirección de Colonial, reflejando claramente su compromiso, apoyo e interés en el desarrollo de una cultura de Seguridad de la Información.

Será responsabilidad de la Dirección difundir los temas relevantes en materia de seguridad.

Las Políticas serán comunicadas a todo el personal y a terceros que presten servicios a Colonial.

Para la difusión interna de los contenidos de las Políticas de Seguridad de la Información se deberán utilizar los medios de que disponga Colonial (intranet, boletín, tablones, etc.), así como instancias o campañas de capacitación llevadas a cabo para este efecto.

2.11 Referencias

Los estándares y mejores prácticas referenciados son los siguientes:

- **ISO/IEC 27002**: Proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información para los responsables de iniciar, implantar o mantener sistemas de gestión de seguridad de la información.

- **NIST Cybersecurity Framework**: Permite a las organizaciones aplicar los principios y las mejores prácticas de gestión de riesgos para la mejora de la seguridad y la resiliencia de las infraestructuras críticas.

- **NIST SP 800-53**: Aporta un catálogo de controles de seguridad para todos los sistemas de información federal de Estados Unidos, exceptuando los relacionados con la seguridad nacional.

3 Documentación relacionada

La documentación relacionada con esta política es la siguiente:

- Código Ético de Inmobiliaria Colonial Socimi S.A.
- Procedimientos y protocolos de Inmobiliaria Colonial Socimi S.A. en materia de protección de datos
- Procedimiento de implantación de plataforma base.
- Procedimiento de uso IRM (*Information Rights Management)*
- Procedimiento de operaciones CPD *(Centro de Proceso de Datos)*