

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Aprobada por el Consejo de Administración de fecha 27 de febrero de 2017

## **I. OBJETO Y ALCANCE**

El objeto de la presente Política, de alcance global, es establecer el marco de seguridad de la información, en el desarrollo de las actividades propias de MELIA HOTELS INTERNATIONAL S.A. y su Grupo (en adelante MHI), basado en las buenas prácticas internacionalmente reconocidas de gestión de la Seguridad de la Información para garantizar en todo momento la confidencialidad, integridad y disponibilidad de la información objeto de tratamiento en cualquiera de sus ámbitos de negocio.

El contenido de la presente Política se establece con carácter de mínimos, sin perjuicio de la regulación adicional y de carácter específico que pueda ser aprobada referente a la materia, y sin perjuicio de las regulaciones legales concretas que puedan resultar de aplicación en cualquiera de los países en los que la Sociedad o cualquier entidad de su Grupo pueda desarrollar actividades.

La presente política fija los objetivos de seguridad e identifica los recursos de tratamiento de la misma, a fin de garantizar el cumplimiento del nivel de protección exigible y refleja el compromiso con respecto a la necesidad de establecer los mecanismos precisos para garantizar el tratamiento confidencial e íntegro de la información, en consonancia con la estrategia de negocio de MHI.

El Consejo, aprobó la Política de Seguridad de la Información de la Compañía en noviembre de 2011, revisando la misma en febrero de 2017.

## **II. MARCO DE APLICACIÓN**

La presente Política se enmarca y aprueba atendiendo, entre otros, a los compromisos contenidos en el Código Ético de Meliá Hotels International S.A. tanto en relación con nuestros clientes (compromiso de protección de la información y datos que los clientes nos confían), como con nuestros accionistas e inversores (asegurar la máxima fiabilidad y exactitud de nuestros registros contables y financieros).

## **III. PRINCIPIOS RECTORES**

MHI es consciente de la necesidad de crear una cultura de seguridad de la información que opere en todos los ámbitos de negocio, tanto interno (en relación con todo el personal) como externo (en relación con los stakeholders) y con una perspectiva global propia de una empresa con presencia internacional.

Siendo este entorno un escenario global y cambiante, la seguridad de la información debe percibirse como un proceso de mejora continua, que permita alcanzar niveles de seguridad cada vez más avanzados, con el objetivo prioritario de garantizar el cumplimiento de la legislación vigente, velando a su vez, por el cumplimiento de todos aquellos otros requerimientos legales o reglamentarios que resulten aplicables en cada país, en concreto se pondrá especial atención a las siguientes materias:

- Protección de Datos de Carácter Personal. La seguridad de la información de nuestros clientes y aquellos stakeholders de los que se traten datos de carácter personal es prioritaria para MHI, para lo cual se dotan las estructuras, planes de seguridad y mecanismos de control para conseguir el alineamiento con la legislación existente en dicha materia en cada país.
- Tratamiento seguro y responsable de datos de tarjetas de crédito y medios de pago. Se realizarán los máximos esfuerzos por imposibilitar su compromiso o filtración. La sociedad y sus empleados se comprometen a utilizar de forma diligente los recursos puestos a su disposición para el tratamiento de la información asociada a los datos de tarjeta de crédito; haciendo uso de los medios que garanticen la máxima seguridad y confidencialidad de los datos, para evitar la utilización fraudulenta de cualesquiera medios y velando por el cumplimiento de la legislación y normativa de aplicación vigente en cada momento. Entre las medidas adoptadas, la sociedad cumple con los estándares de la industria de medios de pago (PCI/DSS) adoptando los estándares de seguridad (PCI/DSS) requeridos a los comerciantes para asegurar la debida protección y confidencialidad de la información de sus clientes.
- Instalación o utilización no autorizada de activos informáticos que puedan atentar contra la propiedad intelectual e industrial. Se promoverá de forma activa la sensibilización y concienciación de los empleados en la abstención de la utilización de los mismos, conforme a la legislación vigente.
- Daños informáticos. La sociedad y sus empleados preservarán el buen uso de los equipos, sistemas y programas informáticos puestos a su disposición, actuando conforme a criterios de seguridad, confidencialidad y eficiencia, excluyendo cualquier acción que sea ilícita o contraria a las normativa vigente en cada país, o que pueda causar daños informáticos en los sistemas de la compañía o de cualquier tercero que se relacione con los mismos, para ello, realiza entre otras, una actividad preventiva de detección de Software malicioso.

-Continuidad de negocio. La sociedad y sus empleados desarrollarán planes y procesos que garanticen las normalidad y continuidad de las operaciones en caso de incidentes informáticos.

- Derechos relativos a la intimidad y acceso no autorizado. La sociedad ha dispuesto de los recursos técnicos, humanos y organizativos necesarios para asegurar la confidencialidad de la información y la implantación de sistemas de control de accesos a los repositorios de información, tales como la administración de identidades o cuentas de usuario.

Por todo ello MHI dispone de los sistemas de control y monitorización técnicos, físicos y organizativos que resultan necesarios para aportar la confidencialidad, integridad y disponibilidad de la información gestionada en el seno de la empresa y su Grupo de forma efectiva.

Los objetivos en materia de seguridad operan por tanto a los más altos niveles de la compañía, ya que suponen un elemento fundamental para la consecución de los objetivos estratégicos de la misma.

Todo lo anterior, sin perjuicio de todos aquellos otros requerimientos legales o reglamentarios, no recogidos expresamente en la presente política y que resulten aplicables en cada país, sobre aquellas materias que afecten de alguna forma a los negocios gestionados por MHI.

La existencia de Normas, procesos, procedimientos y manuales resulta indispensable para ello, como también lo es el compromiso de mantenerlas permanentemente actualizados, para garantizar en todo momento la vigencia y oportunidad de los controles y garantizar su adecuación a las necesidades específicas de MHI.

Se promueve la implicación directa de todos los miembros de la Organización, fomentando una actitud proactiva, crítica y constructiva en permanente búsqueda de la mejora y la calidad en el tratamiento, evolución, seguridad y salvaguarda de la información.

La compañía, comprometida a proporcionar los medios necesarios para la consecución de los objetivos de seguridad establecidos, cuenta con la colaboración de todos los empleados y asume la responsabilidad de la motivación y formación de los mismos en el conocimiento y cumplimiento de esta Política.