Política de Seguridad de la Información

1. Introducción

La presente Política de Seguridad de la Información (en adelante, la "Política") ha sido aprobada por el Comité de Dirección de NH Hotel Group, S.A. (en adelante, “Grupo NH” o “NH”) en septiembre de 2023 y establece las directrices para garantizar la confidencialidad, integridad y disponibilidad de la información objeto de tratamiento en el ámbito de nuestro negocio.

La información es, para NH y para las personas y sociedades que dependen de sus servicios, uno de los activos esenciales para la consecución de sus objetivos de negocio.

Los *team members* y la Dirección del Grupo NH, así como los asociados y terceros que presten sus servicios desarrollando actividades de negocio de NH, están sujetos a las obligaciones derivadas de esta política.

El Grupo NH está comprometido con el cumplimiento de la Política de Seguridad de la Información siguiendo las buenas prácticas y los estándares internacionalmente reconocidos,

2. Objetivos

El objetivo de esta política es definir las líneas de actuación que conforman la estrategia corporativa de NH en materia de seguridad de la información, desarrollando directrices claras y concisas para la gestión, protección y buen uso de los activos de información del Grupo NH.

3. Alcance

El ámbito de aplicación de la política incluye los sistemas de información y comunicaciones, los servicios informáticos y las tecnologías que soportan los procesos, servicios y funciones empresariales del Grupo NH, con independencia de la ubicación de las operaciones de tratamiento o de los soportes o medios que contengan la información.

La presente Política es de aplicación a las siguientes personas, ya sean físicas o jurídicas:

- **Empleados** de todas las sociedades que conformen el grupo NH, con independencia de la modalidad de contrato que rige su relación laboral, del cargo que ostentan o de su ubicación geográfica, incluyendo becarios, así como personas que trabajan en hoteles de la marca NH (por ejemplo hoteles en gestión).
- Directivos de todas las sociedades que conforman el grupo NH, con independencia de la modalidad de contrato que rige su relación, cargo que ostenta o la ubicación geográfica. Las siguientes personas tendrán la consideración en todo caso de Directivos:
  - Administradores/Consejeros de NH y sus filiales,
  - Miembros de la Alta Dirección o de los distintos Comités con los que pudiera contar la Compañía.
- Clientes, proveedores o socios, en la medida en que el presente documento pueda serles de aplicación y NH tenga la capacidad de hacerla efectiva y hacer valer frente a terceros.

Asimismo, la aplicación de la presente Política en todo o en parte se hará extensiva a cualquiera otra persona física y/o jurídica ligada a NH a fin de cumplir con lo dispuesto en la presente Política, siempre y cuando resulte posible su aplicación a terceros, dependiendo de la naturaleza de la relación.

4. Governance

Integrar las consideraciones relacionadas con la seguridad de la información en las decisiones empresariales de la siguiente forma:

- **Consejo de Administración,** máximo órgano de gobierno de NH Hotel Group, es el encargado de aprobar asuntos relacionados con la seguridad de la información, así como el mapa de Riesgos, incluyendo el riesgo de ciber-amenazas.
- **Comité de Dirección,** órgano que garantiza la viabilidad del negocio, involucrado en todas las decisiones relacionadas con la seguridad de la información.
- **Comité Ejecutivo de Seguridad de la Información:** dar seguimiento de los avances y la consecución de los objetivos de la estrategia de ciberseguridad. Capacidad para afrontar los riesgos y oportunidades relacionados así como alentar a la Alta Dirección los problemas relacionados con la seguridad cibernética, así como priorizarlos y supervisarlos.
- **Chief Operations Officer & Global Transformation Leader:** responsable de supervisar la Estrategia de ciberseguridad y de comunicar los asuntos materiales relacionados con la ciberseguridad a la Alta Dirección. Asimismo, lidera el Comité Ejecutivo de Seguridad de la Información.
- **CISO (Information Security Officer):** ejecutivo de alto nivel, que vela por la ciberseguridad de NH y garantiza que las tecnologías y los activos de información estén protegidos ante posibles ciberataques y/o fugas de datos. Asimismo, es el responsable de establecer y dar seguimiento a la estrategia de ciberseguridad de NH. Asimismo, forma parte del Comité de Seguridad de la Información.
- **Departamento IT& Systems**: coordinar las cuestiones relacionadas con la ciberseguridad, así como implantar soluciones que combinen seguridad, sostenibilidad y eficiencia. Identificar, evaluar y mitigar posibles riesgos relacionados con la ciberseguridad que puedan afectar a la viabilidad del negocio.

Adicionalmente, 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.

NH, 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. Asimismo, la Dirección de NH se compromete a apoyar su implantación y difusión.

5. Compromisos

La Dirección de NH está comprometida con la gestión de la seguridad de la información y establece los objetivos, responsabilidades y comportamientos necesarios.

La Dirección de NH es responsable de promover y apoyar el establecimiento de medidas técnicas, organizativas y físicas que garanticen la integridad, disponibilidad y confidencialidad de la información de NH, con el fin de evitar posibles amenazas internas o externas. La Dirección de NH es responsable de proporcionar los recursos necesarios para el establecimiento de la estructura organizativa, procesos, procedimientos y medidas que

garanticen el cumplimiento de las leyes y reglamentos aplicables, así como la correcta gestión de la seguridad de la información.

6. Principios de Seguridad de la Información

La política se desarrolla y aplica a través de las siguientes directrices:

- Alineamiento estratégico y visión de futuro: Todos los miembros de la organización deben considerar la ciberseguridad un elemento fundamental para la protección del negocio y su continuidad. Se deben establecer planes a corto, medio y largo plazo, de manera transversal, para lograr la consecución de los objetivos y la mejora continua de la ciberseguridad.
- Organización de la seguridad de la información: La aplicación de medidas organizativas y técnicas de seguridad debe contemplarse para todos los activos de información de NH, con independencia del soporte físico en el que se encuentren y del lugar desde el que se procesen. Esto debe ser llevado a cabo por un equipo debidamente cualificado, y dotado de una adecuada asignación de recursos, bajo la dirección del Chief Information Security Officer (CISO). Además, se debe reportar periódicamente la situación de la ciberseguridad de la organización a los órganos de gobierno.
- Seguridad de los recursos humanos: Deben establecerse mecanismos para concienciar a todo el personal de NH en materia de seguridad de la información.
- Gestión de activos: Los activos de información deben clasificarse y se asignarán responsabilidades sobre los mismos.
- Control de acceso: Los usuarios deben tener acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones. Los usuarios deben ser responsables de la confidencialidad de la información de NH y de sus credenciales de acceso.
- Criptografía: Las claves criptográficas bajo responsabilidad de NH deben estar protegidas.
- Seguridad física y ambiental: Los activos de información deben estar ubicados en zonas seguras, protegidos por controles de acceso físico y sistemas de protección ambiental.
- Seguridad de las operaciones: Deben establecerse procedimientos formalizados para la gestión y explotación seguras de los sistemas de información y la infraestructura tecnológica de NH. Deben llevarse a cabo evaluaciones periódicas de la seguridad para anticipar la detección de vulnerabilidades antes de que puedan ser explotadas y para fomentar la mejora continua.
- Seguridad de las comunicaciones: Las redes de comunicaciones deben diseñarse e implementarse para garantizar la transferencia segura de información, y para cumplir con el principio de exposición mínima de acuerdo con la gestión de riesgos.
- Adquisición, desarrollo y mantenimiento de sistemas: La seguridad de la información debe considerarse parte de la actividad habitual, estando presente desde la fase de diseño de cualquier proyecto.
- Relaciones con los proveedores: Deben existir procedimientos para garantizar que los terceros, que estén relacionados con NH y que traten con activos de información de NH, cumplan con la política.
- Gestión de incidentes de seguridad de la información: Deben definirse procedimientos para detectar y responder a incidentes que puedan afectar a la seguridad de la información de NH, con el objetivo de ser resilientes operativamente.
- Gestión del riesgo: La gestión, evaluación y comunicación del riesgo de ciberseguridad debe ser un elemento clave en la gestión del riesgo corporativo para toda la organización.
- Aspectos de seguridad de la información de la gestión de la continuidad del negocio: Deben establecerse controles preventivos y reactivos para garantizar la disponibilidad de los recursos de información críticos para el negocio.

- Cumplimiento y buenas prácticas: Se debe garantizar que los sistemas de información y las operaciones de tratamiento realizadas por NH cumplen con la legislación vigente y están alineados con las guías de buenas prácticas y los estándares en materia de ciberseguridad.

7. Estructura

El conjunto de documentos normativos se estructura en el siguiente modelo jerárquico de cuatro (4) tipologías de documentos normativos:

- Política: el presente documento normativo, que establece los principios de seguridad de la información que deben desarrollarse en los documentos de los siguientes niveles jerárquicos.
- Normas: Documentos normativos en los que se definen los objetivos de control, desarrollando cada uno de los principios de seguridad de la información detallados en la política.
- Procedimientos: Documentos normativos en los que se determinan las acciones concretas a realizar para implantar los objetivos de control definidos en las normas. Estos documentos normativos emanan de las normas o de otros procedimientos.
- Instrucciones de trabajo: Documentos normativos que determinan cómo aplicar los requisitos de seguridad de la información. Esta categoría también incluye manuales, formularios y plantillas, entre otros. Estos documentos emanan de procedimientos u otras instrucciones técnicas de trabajo.

Todas las tipologías de normas reglamentarias mencionadas son de obligado cumplimiento.
Las normas que contradigan una norma de rango superior carecerán de validez.

8. Monitorización y canal de información

La política debe darse a conocer a todos los usuarios de los sistemas de información y comunicaciones de NH.
La política debe darse a conocer a través del Portal del Empleado de NH.

Las entidades que procesen información propiedad del Grupo NH o bajo su responsabilidad, en el contexto de una relación laboral o comercial, deben adherirse a la Política, reconocer su responsabilidad de cumplir con la misma y, garantizar el cumplimiento de los requisitos de seguridad de la información aplicables.

Todos los usuarios deben expresar la comprensión de sus obligaciones en relación con la política.

Los incidentes y las solicitudes de información adicional sobre la política pueden comunicarse a Seguridad de la Información a través del correo electrónico infosec@nh-hotels.com.

9. Cumplimiento

Todos los empleados, así como asociados internos y externos de NH Hotel Group son responsables de garantizar el cumplimiento de los principios de la Política y de los documentos normativos internos de NH que emanan de la Política, así como de las leyes y reglamentos vigentes en materia de seguridad de la información.

La actividad de los usuarios en los sistemas de información, donde se procesa información propiedad de NH o bajo su responsabilidad, debe ser monitorizada y registrada con el fin de garantizar el correcto uso de los sistemas de información y prevenir incidentes de seguridad de la información que puedan poner en peligro la seguridad de los activos de información de NH.

La política proporciona un marco para los aspectos cubiertos por las siguientes normas de seguridad de la información reconocidas internacionalmente:

- Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos (ISO/IEC 27001).
- Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para los controles de seguridad de la información (ISO/IEC 27002)
- Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS).

Para el desarrollo de la política se han tomado como referencia los requisitos legales establecidos en las leyes y reglamentos de los estados en los que opera el Grupo NH, tales como el GDPR y las leyes nacionales sobre propiedad intelectual (PI). La legislación y normas sobre seguridad de la información incluidas en el ámbito de aplicación de la política se han detallado en el Marco de Seguridad de la Información. Asimismo, se han tenido en consideración las recomendaciones contenidas en el Código de Buen Gobierno de la Ciberseguridad del Foro Nacional de Ciberseguridad.

Teniendo en cuenta que NH Group opera en diferentes países, en caso de que el contenido de la política difiera de las leyes y normativas nacionales, se aplicarán las medidas y controles de la norma más estricta.

NH se reserva el derecho de emprender acciones legales o disciplinarias en situaciones de incumplimiento de la política.

10. Documentación relacionada

- Código de Conducta de NH Hotel Group, S.A.
- Política de Privacidad de NH Hotel Group, S.A
- Política de Sostenibilidad de NH Hotel Group, S.A
- Política de Derechos Humanos de NH Hotel Group, S.A.
- Código de Conducta Coperama
- Compromiso de Compras Sostenibles de NH Hotel Group, S.A.

Adicionalmente, la Compañía cuenta con dos marcos normativos de seguridad de la información que complementan a la presente política e impulsan su correcta implementación:

- ALLNH-NOR201-ES - Glosario de términos y definiciones
- ALLNH-NOR202-ES - Marco Normativo de Seguridad de la Información

11. Control de versiones

Versión	Revisado por	Aprobado por	Fecha

1.0	Departamento de Tecnología de la Información	Comité de Dirección	Diciembre 2013
1.1	Departamento de Tecnología de la Información	Comité de Dirección	Abril 2015
1.2	Departamento de Tecnología de la Información	Comité de Dirección	Junio 2018
1.3	Departamento de Tecnología de la Información	Comité de Dirección	Noviembre 2018
1.4	Departamento de Tecnología de la Información	Consejo de Administración	Noviembre 2023