DOCUMENTO DE SEGURIDAD

Anexo XI – CONTROL DE ACCESO FÍSICO

CONFIDENCIAL

Nivel de seguridad de la información:

Uso Interno

Localización: Departamento de Sistemas

DERECHOS DE USO:

El presente documento es propiedad de NH Hotel Group, tiene carácter de interno y no podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquiera otro fuera del ámbito de NH Hotel Group. Asimismo tampoco podrá ser objeto de préstamo, alquiler o cualquier forma de cesión de uso sin el permiso previo y escrito de NH Hotel Group, titular del copyright. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será perseguida conforme a ley

Revisiones del Documento

Versión	Fecha	Elaborado por	Revisado por	Aprobado por
1.0	Noviembre 2015	Deloitte	Auditoría Interna y Seguridad de la Información	Asesoría Jurídica

Control de Cambios:

Versión	Fecha de modificación	Revisado por

CONFIDENCIAL

Índice

1. INTRODUCCIÓN 4

2. IDENTIFICACIÓN 5

3. AUTENTICACIÓN 6

4. AUTORIZACIÓN 7

5. ACTIVIDADES DE CONTROL 8

CONFIDENCIAL

1. Introducción

El objetivo de este anexo del Documento de Seguridad es describir las políticas y procedimientos existentes en NH Hotel Group, referentes al control de acceso físico a las diferentes instalaciones.

La Compañía cuenta con un número relevante de CPDs, de distinta relevancia entre sí:

- Por un lado, el CPD principal y el CPD secundario (donde reside la lógica principal de procesamiento de NH para España) están ubicados en instalaciones de Telefónica, y el control de acceso a los mismos está regulado por esta compañía, que cuenta con certificaciones que acreditan su seguridad.

- Por otro lado, los Head Quarters de Madrid, en Santa Engracia 120, cuentan a su vez con un CPD donde también reside información de carácter personal. Su control de acceso está regulado por parte de personal de NH.

- Además, en las oficinas de Barcelona (Hospitalet) se cuenta con una sala técnica en la que se cuenta con servidores de ficheros que pueden contener información de carácter personal.

- Las oficinas de la BU de España, en Madrid (Alfonso Gómez) cuentan a su vez con una sala técnica para alojar sus sistemas locales, y donde también existen servidores de ficheros con información personal de los departamentos en él incluidos.

- De igual forma, el Call Center para España está ubicado en Madrid, y cuenta también con una sala técnica, si bien su gestión y control son responsabilidad de Telefónica.

- Por último, el conjunto de hoteles de la Compañía están equipados con pequeñas salas técnicas, si bien la presencia de información de carácter personal en las mismas es limitada.

En todos los casos, el acceso a estas salas está restringido al personal autorizado a tal efecto (si bien las medidas en cada caso existentes son distintas, en función de la criticidad de los sistemas que en su interior se incluyen).

El responsable de seguridad realizará un control periódico sobre el cumplimiento del procedimiento de control de accesos físicos a los principales centros de procesamiento, con el objetivo de verificar y detectar posibles incidencias de seguridad, de lo cual mantendrá un registro.

CONFIDENCIAL

2. Identificación

El acceso a las dependencias donde NH haya dispuesto equipos para el tratamiento automatizado de información deberá estar controlado en todo momento. Por ello, toda persona, ajena o no a la empresa, deberá identificarse para poder acceder a las instalaciones donde se encuentren albergados los sistemas para el tratamiento automatizado de la información.

Bastará con cualquier acreditación oficial para el acceso físico (DNI / Pasaporte) y deberá existir un registro de entradas y salidas junto con el motivo del mismo, según se describe en el apartado.

De la misma manera se deberá garantizar el control de acceso a aquellas dependencias donde se almacene información en formato papel en las mismas condiciones.

CONFIDENCIAL

3. Autenticación

Deberán existir medidas adicionales de seguridad en los accesos a dependencias que alberguen equipos críticos para el tratamiento de la información del grupo (Centros de Procesamiento de Datos, CPDs), mediante el establecimiento de un nivel adicional de identificación y autenticación. Para ello, se instalarán mecanismos como llaves, teclados numéricos, tarjetas, sistemas de identificación biométrica, etc., que garanticen que el acceso a esas dependencias se lleva a cabo por personal autorizado. Se garantizará en todo momento que las medidas establecidas son acordes con la sensibilidad de la Información a proteger.

CONFIDENCIAL

4. Autorización

La autorización a CPD's de la compañía debe contar con una doble autorización siendo obligatoria la presencia de personal autorizado de NH, exceptuando aquellos colaboradores externos que tengan acordado lo contrario (por ejemplo: personal en el que se haya externalizado la administración del sistema).

Los accesos a los lugares en los que se ubiquen servidores, electrónica de red, distribución de cableado, sistemas de alimentación ininterrumpida y/o soportes de información deberán tener controlado el acceso físico de cualquier persona. Para ello, el área de explotación de sistemas llevará un registro automatizado de los accesos a tales dependencias. En ese registro, deberán quedar reflejados, como mínimo, los siguientes datos del visitante o visitantes:

- Nombre y Apellidos del visitante.
- Empresa.
- Motivo de la visita.
- Fecha / Hora.

El acceso a estas dependencias se realizará con un propósito único y específico, independientemente del número de personas que vayan a cumplir con ese propósito. Así, no podrán confluir cometidos distintos en el mismo momento, garantizándose la delimitación de las responsabilidades.

CONFIDENCIAL

5. Actividades de control

Derivados de este procedimiento se extrae la siguiente actividad de control:

- Se deberá actualizar el documento **A11.1 - Accesos autorizados al CPD (registro)** cada vez que se produzca un cambio en la distribución de accesos a cada uno de los centros de proceso de datos de la organización (internos y externos).

  Cada seis meses el Responsable de Seguridad validará que el fichero haya sido adecuadamente actualizado.

CONFIDENCIAL