DOCUMENTO DE SEGURIDAD

Anexo XIV – TELECOMUNICACIONES

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

Índice

1. INTRODUCCIÓN 4

2. MEDIDAS DE SEGURIDAD EN LAS TELECOMUNICACIONES DE NH HOTEL GROUP 5

3. MEDIDAS DE SEGURIDAD EN LA TRANSMISIÓN DE FICHEROS 6

4. REGISTRO DE LAS OPERACIONES 7

5. REVISIONES PERIÓDICAS 8

1. Introducción

Esta sección describe los mecanismos establecidos para garantizar la confidencialidad e integridad en el envío y recepción telemática de información a través de redes de telecomunicaciones que atendiendo a su naturaleza requieren medidas de seguridad de nivel alto.

La transmisión de datos por red, ya sea por medio de correo electrónico o mediante sistemas de transferencia de ficheros, se está convirtiendo en uno de los medios más utilizados para el envío de datos, hasta el punto de que está sustituyendo a los soportes físicos. Por ello merecen un tratamiento especial ya que, por sus características, pueden ser más vulnerables que los soportes físicos tradicionales.

2. Medidas de seguridad en las telecomunicaciones de NH Hotel Group

En NH se han establecido una serie de medidas tecnológicas que permiten garantizar la confidencialidad, integridad y disponibilidad de la información que se gestiona tanto internamente como la que se intercambia con clientes, proveedores, etc.

A nivel perimetral se cuentan con diversas capas de firewalls, WAF e IPS, los flujos de información internos entre las diferentes sedes, hablando tanto de oficinas como de hoteles, se basan en una red de comunicaciones MPLS. Para las comunicaciones de proveedores externos a recursos internos, éstas se han de realizar a través de conexión VPN necesitando un doble factor de autenticación para poder realizarse de manera correcta.

Se ha establecido un sistema de monitorización de los diferentes elementos de seguridad y de manera recurrente en el tiempo se realizan escaneos de intrusión sobre los puntos de acceso.

3. Medidas de seguridad en la transmisión de ficheros

NH ofrece a los empleados un paquete de herramientas que incluye la posibilidad de cifrado de información. El objetivo es preservar la confidencialidad de los ficheros de nivel alto transmitidos a través del correo electrónico.

Para la transmisión de ficheros de nivel alto (ver anexo **A05.3 Ficheros lógicos (catálogo)**) la información será enviada a través de la herramienta corporativa *SendYourFiles* o a través de correo comprimiendo la información con contraseña y facilitando la contraseña en un email posterior (ver **A14.1 – Salidas telemáticas (registro)**).

4. Registro de las operaciones

No podrán realizarse extracciones de ficheros de carácter personal sin la autorización por parte del Responsable del Fichero. Dicha aprobación deberá ser expresa en lo relativo a los ficheros de nivel alto.

Se ha habilitado un registro de envíos telemáticos para documentar dichas operaciones (ver **A14.1 – Salidas telemáticas (registro)**).

En el supuesto de que el envío telemático responda a una práctica periódica, podrá documentarse mediante una autorización genérica en el citado registro (en el resto de casos, donde de manera puntual se procede al envío, estos deberán ser sistemáticamente documentados).

5. Revisiones Periódicas

Se deberá comprobar periódicamente que:

- Las salidas de nivel alto estén correctamente cifradas tal y como se indica en el apartado 2 de este documento.

- Las salidas de nivel alto estén correctamente registradas tal y como se indica en el apartado 3 de este documento.

Para mayor detalle, ver **A03.1 - Actividades de control periódicas (catálogo)**.