DOCUMENTO DE SEGURIDAD

Anexo IV – IDENTIFICACIÓN Y AUTENTICACIÓN

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

2.1 INTEGRIDAD DE LOS IDENTIFICADORES 5
2.2 NOMENCLATURA 5

3. AUTENTICACIÓN 6

3.1 CONFIDENCIALIDAD DE LAS CONTRASEÑAS 6

4. PROCEDIMIENTO DE ASIGNACIÓN Y DISTRIBUCIÓN DE CONTRASEÑAS 8

5. RELACIÓN DE USUARIOS 9

CONFIDENCIAL

1. Introducción

El objetivo de este anexo del Documento de Seguridad es describir las políticas y procedimientos existentes en NH Hotel Group, referentes a Identificación y Autenticación de los usuarios. Los procedimientos específicos para los sistemas que manejan información confidencial de la Compañía, quedan recogidos en el documento **A05.1 - Características técnicas y de seguridad de las aplicaciones informáticas (catálogo)**.

CONFIDENCIAL

2. Identificación

NH Hotel Group dispone de mecanismos de identificación para el acceso de los usuarios a la información de carácter personal existente en los sistemas informáticos de NH Hotel Group, estableciendo las siguientes normativas con respecto la identificación de usuarios:

2.1 Integridad de los Identificadores

NH Hotel Group cuenta con medidas de seguridad que aseguran un control sobre los permisos de acceso de los usuarios a los sistemas. De este modo, existen procesos que controlan el tiempo máximo de inactividad de los usuarios.

Todas las características de seguridad de los sistemas de información que contienen datos de carácter personal están recogidas en el anexo **A05.1 - Características técnicas y de seguridad de las aplicaciones informáticas (catálogo).**

2.2 Nomenclatura

La Compañía ofrece a los usuarios de las aplicaciones un identificador único, a través del cual es posible identificar al responsable de las cuentas.

Asimismo, los usuarios genéricos de las aplicaciones quedan controlados al asignarse un responsable de su uso.

En el documento **A04.1 - Accesos autorizados por fichero (catálogo)** se incluyen los listados de usuarios por aplicación, las revisiones de usuarios genéricos llevadas a cabo, y los resultados obtenidos. Por otro lado, en el documento **A05.2 - Usuarios genéricos controlados (registro)** se recogen los usuarios genéricos identificados y controlados por la Compañía.

CONFIDENCIAL

3. Autenticación

Los identificadores llevarán asociada una clave de acceso que garantice que el uso de los mismos tiene lugar por la persona registrada. Para ello, se establecen una serie de requisitos de calidad a la hora de definir la clave de acceso:

- Contraseñas de Usuario

Las contraseñas deberán cumplir una serie de requisitos en cuanto a su longitud, caducidad, periodicidad de renovación, etc. Estos requisitos se pueden encontrar en el anexo **A05.1 - Características técnicas y de seguridad de las aplicaciones informáticas (catálogo)**.

3.1 Confidencialidad de las Contraseñas

Las consecuencias que se deriven del incumplimiento de las normas establecidas en este punto serán de exclusiva responsabilidad del propietario del identificador y contraseña de usuario.

Los responsables de cada departamento deberán velar por el cumplimiento de esta norma en el ámbito de su responsabilidad, exigiendo a sus subordinados el acatamiento de la misma y comunicando los incumplimientos al Responsable de Seguridad como incidencias de seguridad.

Las normas a seguir con respecto la confidencialidad de las contraseñas, son:

- Las contraseñas no se guardarán en un fichero en claro sino que se almacenarán cifradas de forma robusta o mediante funciones resumen en un fichero de acceso restringido, de forma que se garantice su confidencialidad e integridad. Así mismo, tampoco podrán ser visualizadas en claro en la pantalla tanto al introducirlas cómo en caso de recuperarlas.
- Los ficheros que contienen las contraseñas de usuarios de acceso a los sistemas y aplicaciones deben tener un nivel de protección elevado. Asimismo, las contraseñas de usuarios se protegen ante el uso de mecanismos que puedan violar su confidencialidad tales como el uso de diccionarios, etc.
- Se adoptará un procedimiento de custodia de contraseñas para las cuentas de especial importancia, incluyendo los identificadores de administración, los pertenecientes a mecanismos o secuencias de autenticación de acceso automático, y las claves de los dispositivos de cifrado por las redes de comunicaciones.
- Los sistemas de información ofrecerán mecanismos que permitan el cambio de contraseña en cualquier momento, de manera que cumplan las siguientes funcionalidades:
  - ✓ Se pedirá la contraseña antigua antes de continuar con el mecanismo de cambio de contraseña.
  - ✓ Se pedirá confirmación de la nueva contraseña antes de proceder al cambio (para evitar posibles errores de escritura).
  - ✓ Las contraseñas no se visualizarán en pantalla durante la introducción de las mismas.

CONFIDENCIAL

- Los usuarios dados de alta en los sistemas y aquellos que solicitan cambio por olvido o bloqueo de usuario, serán informados por el administrador del sistema de que la cuenta será desbloqueada, sin necesidad de modificaciones en la contraseña.
- Cuando se informa sobre un olvido de contraseña o bloqueo de usuario (por intentos erróneos reiterados de acceso al sistema) al administrador del sistema, éste deberá tomar las precauciones necesarias para comprobar la identidad del solicitante. En caso de que el bloqueo no haya sido producido por el propietario del identificador de usuario, se debe registrar la incidencia (ver **Anexo X.- Registro de Incidencias**).
- Los usuarios deberán cambiar su contraseña si existen indicios de que la misma puede ser conocida y utilizada por otras personas.
- Cada usuario es responsable de la confidencialidad de su contraseña de acceso, por lo que se prohíbe su comunicación o cesión a cualquier otra persona, incluidos compañeros, superiores o el propio Departamento de Tecnología y Sistemas. Se considerará al usuario, responsable de las actividades sobre el sistema y aplicaciones realizadas con su identificador.
- Las contraseñas no deberán anotarse o guardarse en lugares visibles o fácilmente accesibles como monitores, calendarios de mesa, parte inferior de los teclados, cajoneras, etc.

CONFIDENCIAL

4. Procedimiento de asignación y distribución de contraseñas

Para el acceso a los sistemas, la contraseña inicial se generará de forma automática, tomando como entrada el Nombre y Apellidos y la fecha de alta del usuario en cuestión. Dicha contraseña se generará expirada, obligando al usuario a cambiarla en el primer acceso al sistema.

CONFIDENCIAL

5. Relación de usuarios

NH Hotel Group, con objeto de cumplir el artículo 11.1 del Reglamento de Seguridad, dispone de los mecanismos necesarios para obtener una relación o inventario general actualizado de usuarios con acceso a los datos de carácter personal.

Se dispone de un registro centralizado con todos los usuarios y los accesos y autorizaciones, para poder gestionar los identificadores y las autorizaciones de todo el personal que acceda a los sistemas de NH. Para más información, ver el documento **A04.1 - Accesos autorizados por fichero (catálogo).**

CONFIDENCIAL