DOCUMENTO DE SEGURIDAD

Anexo VII – FICHEROS TEMPORALES

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. NORMATIVA 5

3. PROCEDIMIENTO PARA CONTROL DE FICHEROS TEMPORALES: 6

3.1 EXTRACCIONES DE UNA BASE DE DATOS Y APLICACIONES 6
3.2 FICHEROS GENERADOS EN COLAS DE IMPRESIÓN 6
3.3 FICHEROS CREADOS POR LOS USUARIOS 6
3.4 CONTROLES PERIÓDICOS SOBRE LOS FICHEROS TEMPORALES EN SISTEMAS DE INFORMACIÓN. 7
3.5 CONTROLES PERIÓDICOS SOBRE LOS FICHEROS TEMPORALES NO AUTOMATIZADOS. 7

CONFIDENCIAL

1. Introducción

Un fichero temporal es aquel distinto del original cuya finalidad es un procesamiento paralelo de los datos originales sin afectar al fichero original.

Durante la ejecución del trabajo diario se generan ficheros temporales cuya finalidad es el procesamiento paralelo de los datos originales sin afectar al fichero original. El objetivo del presente anexo del Documento de Seguridad es describir todos los procedimientos que NH Hotel Group desarrolla para garantizar el control y buen uso de los mencionados ficheros.

Mediante las medidas establecidas en el presente documento, todo fichero temporal es borrado o destruido una vez que ha dejado de ser necesario para la finalidad para el cual fue creado.

Según la naturaleza de los ficheros temporales, estos son tratados de distintas formas:

- Las aplicaciones ejecutadas en cada uno de los diferentes entornos suelen generar ficheros temporales locales para su funcionamiento. Estas aplicaciones son las encargadas de crearlos cuando los requieren y eliminarlos cuando ya no son necesarios.
- Los usuarios obtienen ficheros temporales desde los datos contenidos en las aplicaciones principales, con la intención de utilizarlos para una finalidad específica (p.ej. elaboración de informes a la Dirección) durante un período de tiempo limitado.

  Estos ficheros suelen ser almacenados en sus propios ordenadores personales (PCs o equipos portátiles) o bien en las carpetas personales de red, de manera que se asegura su protección contra accesos no permitidos.
- Los usuarios recaban información directamente del usuario y la almacenan en ficheros temporales durante un periodo de tiempo limitado y cuando este periodo se finaliza se procede a destruir la información no original.
- Los usuarios generan ficheros temporales mediante fotocopias o similar de los documentos originales para la realización de un trabajo temporal o auxiliar. Una vez que ya no necesitan estos ficheros temporales, es el propio usuario el encargado de destruirlo

CONFIDENCIAL

2. Normativa

Los usuarios sólo podrán crear ficheros que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco de los puestos PC de usuario si no que serán ubicados en directorios estructurados de los recursos compartidos de los servidores.

En el caso de los ficheros temporales no automatizados, se ubicarán en salas de acceso restringido al personal autorizado, siendo el Responsable de Seguridad el encargado de supervisar y validar que las medidas de control de acceso en los dispositivos de almacenamiento son adecuadas. Las llaves de los armarios donde se guarden los ficheros temporales no automatizados deben ser retiradas de estos al acabar la jornada laboral o durante la jornada laboral en periodos de ausencia significativos. Estas llaves deberán ser custodiadas por la persona responsable de cada armario o sala. En caso de que los armarios o salas sean comunes para varias personas, se designará un responsable del mantenimiento de las llaves, estando esta asignación recogida formalmente.

Por aplicación de las normativas de Seguridad de NH Hotel Group:

- Estos ficheros temporales deben ser borrados por el propio usuario cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

- Debe cumplir las medidas de seguridad que les corresponda según la información que contienen.

Además, ante posibles fallos en los procesos de eliminación de los ficheros temporales, en el caso de los ficheros temporales automatizados, el administrador de cada uno de los sistemas revisara de forma periódica los ficheros / librerías / carpetas, con el fin de borrar todos aquellos ficheros temporales que no hubieran sido eliminados y que ya no fueran necesarios.

CONFIDENCIAL

3. Procedimiento para control de ficheros temporales:

3.1 Extracciones de una base de datos y aplicaciones

En el caso particular de creación de un soporte (CD/DVD) con datos de carácter personal se seguirá el siguiente procedimiento:

En primer lugar es necesario solicitar la creación del fichero mediante incidencia en ServiceDesk, que deberá pasar por la aprobación del Responsable del Tratamiento del Fichero.

El personal de IT es el encargado de garantizar el nivel de seguridad.

Como medida de control adicional, otro técnico del mismo departamento se encarga, una vez al mes, de limpiar esta ubicación de todos los ficheros creados para tal fin.

3.2 Ficheros generados en colas de impresión

Como norma general y siempre que la aplicación lo permita, se utilizara un recurso compartido de los sistemas de información como repositorio de trabajo temporal de dichas aplicaciones.

Dado que de forma general la creación y destrucción de este tipo de ficheros es gestionada automáticamente desde dichas aplicaciones, como segunda medida de control se seguirá el procedimiento general para control de ficheros temporales establecido.

3.3 Ficheros creados por los usuarios

Cada empleado debe realizar un uso adecuado y responsable de las fotocopiadoras, impresoras, fax…, de tal modo que se tengan presentes los siguientes aspectos:

- Cada vez que un usuario imprime un documento debe proceder a recogerlo en ese mismo momento.
- Al acabar la jornada laboral no debe quedar ningún documento en la bandeja de las impresoras.

CONFIDENCIAL

- No se debe proceder a imprimir ningún documento que no sea estrictamente necesario, y se debe tener en cuenta que una vez impreso el documento se le deberán aplicar las medidas que le correspondan acorde a su naturaleza.

- La ubicación de estos dispositivos debe favorecer que se encuentren en todo momento controlados por el personal del Departamento.

3.4 Controles periódicos sobre los ficheros temporales en sistemas de información.

Se entiende como obligación del personal, borrar periódicamente los ficheros que contengan datos de carácter personal que se localicen en los servidores de bases de datos o unidades de red, una vez desaparecida la finalidad perseguida en la creación del fichero y no siendo necesaria su conservación. Previa a la comunicación de esta última circunstancia al Responsable de Seguridad Técnico y siguiendo el procedimiento habilitado para ello con relación a la supresión de ficheros temporales.

3.5 Controles periódicos sobre los ficheros temporales no automatizados.

Para validar que los miembros de NH Hotel Group aplican adecuadamente el procedimiento de gestión de ficheros temporales en soportes no electrónicos, el personal del área de seguridad procederá de forma rutinaria a inspeccionar las áreas comunes, procediéndose a retirar el papel que se encuentre en las zonas de reproducción y que no haya sido recogido. La información que se retire no será destruida de forma inmediata, pero pasado un tiempo prudencial se procederá a su eliminación. Ver **A03.1 - Actividades de control periódicas (catálogo)**.

CONFIDENCIAL