DOCUMENTO DE SEGURIDAD

Anexo I – DIVULGACIÓN DE LAS NORMAS DE SEGURIDAD

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

CONFIDENCIAL

1. Introducción

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar.

El día 19 de abril de 2008, entró en vigor el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD y que deroga el Real Decreto 994/1999 por el cuál quedaba aprobado el Reglamento de Medidas de Seguridad de los Ficheros Automatizados de Datos de Carácter Personal.

El nuevo Reglamento dota de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva y desarrolla los aspectos novedosos de la Ley Orgánica 15/1999, junto con aquellos en los que la experiencia recogida ha aconsejado un cierto de grado de precisión que dote de seguridad jurídica al sistema.

Con la aparición del Nuevo Reglamento, el NH Hotel Group se plantea la necesidad de adaptar, a dicho Reglamento, sus actuales medidas de seguridad sobre los ficheros con datos de carácter personal, para así cumplir con los preceptos establecidos en la LOPD y en el Real Decreto 1720/2007.

Las personas con acceso a los datos de carácter personal y a los sistemas de información de NH Hotel Group, deben ser conscientes de la necesidad de preservar la información y de las consecuencias que acciones inapropiadas en este sentido pueden ocasionar a NH Hotel Group. Es por ello, que el personal con acceso a los datos de carácter personal y a los sistemas de información del NH Hotel Group, es informado de todas las normas de seguridad que afectan al desarrollo de sus funciones, así como de las consecuencias en que pudiera incurrir en caso de incumplimiento.

El conocimiento y cumplimiento de estas normas afecta a todos los usuarios y empleados de NH Hotel Group que intervengan, de forma directa o indirecta, en el tratamiento de datos de carácter personal.

CONFIDENCIAL

2. Disposiciones Generales

Las medidas de seguridad que se contemplan en dicho Reglamento establecen tres niveles diferentes - Básico, Medio y Alto - dependiendo de la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad e integridad de la información. Así en el Reglamento se considera,

- **Nivel Básico -** aplicable a todos los ficheros con datos de carácter personal.
  - Como excepción solo se aplicaran las medidas de nivel básico (a ficheros considerados inicialmente como nivel alto) en los siguientes supuestos:
    - Ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual cuando:

      a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

      b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

    - Ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado,

- **Nivel Medio -** aplicable a ficheros con datos:

  a) Relativos a la comisión de infracciones administrativas o penales.

  b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la LOPD (ficheros de solvencia patrimonial y crédito).

  c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

  d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

  e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

  f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan

CONFIDENCIAL

evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

- **Nivel Alto -** aplicable a ficheros que**:**

  a) Se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

  b) Contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

  c) Aquéllos que contengan datos derivados de actos de violencia de género.

  d) A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización. Se les aplicara las medidas de seguridad de nivel alto contenida en el artículo 103 del reglamento.

Es importante hacer constar que cada uno de los niveles descritos anteriormente debe incorporar las medidas de seguridad de los niveles inmediatamente inferiores. Así, aquellos ficheros calificados de Nivel Alto deberán reunir las medidas de seguridad correspondientes a los niveles: Básico, Medio y Alto.

Ante una inspección de la Agencia Española de Protección de Datos (en adelante AEPD), las unidades de NH Hotel Group deberán tener perfectamente identificados los ficheros de los que sean responsables y que contengan datos de carácter personal, las medidas de seguridad en los accesos a dichos ficheros, la relación de usuarios que acceden a los mismos y las funciones y obligaciones de cada una de las personas que acceden a datos de carácter personal.

CONFIDENCIAL

3. Medidas De Seguridad

El desarrollo de las medidas de seguridad, ajustadas al Reglamento, comprende la elaboración de un Documento de Seguridad que será de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.

Dicho documento contiene, entre otros, los siguientes aspectos:

- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad que exige este Reglamento.
- Definición de funciones y obligaciones del personal con acceso a los datos de carácter personal y a los sistemas de información.
- Procedimiento de notificación, gestión y respuesta ante incidencias que pudieran afectar a la seguridad de los datos de carácter personal.
- Procedimientos de identificación, autenticación y control de acceso de los usuarios a los sistemas de información.
- Políticas de realización de copias de seguridad, procedimientos de recuperación y gestión de soportes informáticos que contengan datos de carácter personal.

El Reglamento de Medidas de Seguridad obliga a identificar una serie de responsables en relación con el tratamiento de los ficheros que contienen datos de carácter personal.

Así, en el NH Hotel Group se ha identificado como responsable de los ficheros declarados a la Agencia de Protección de Datos al NH HOTEL GROUP, y se han identificado Responsables de Tratamiento de cada uno de los ficheros declarados, los cuáles serán los encargados de decidir sobre la finalidad, contenido y uso de los mismos.

De forma general, las funciones de los Responsables de Tratamiento serán, entre otras, las siguientes:

- Decisión sobre el uso, aprovechamiento y contenido del fichero.
- Mantenimiento de una relación actualizada de usuarios con acceso autorizado al fichero.
- Gestión de las altas, bajas y modificaciones de los accesos autorizados al fichero
- Autorización de la salida, fuera del local de ubicación del fichero, de soportes informáticos que contengan datos de carácter personal

CONFIDENCIAL

- Coordinación con el Responsable de Seguridad de toda la problemática que afecte a la seguridad del fichero.

La modificación o creación de ficheros que contengan datos de carácter personal deberá comunicarse a Asesoría Jurídica, quienes deberán comunicarlo al Responsable de Seguridad de forma que se puedan implantar las medidas técnicas y organizativas adecuadas al nivel de los datos gestionados.

El Responsable de Seguridad del NH Hotel Group, será el responsable del seguimiento del cumplimiento de la normativa en cuanto al acceso y el uso correcto de la información.

CONFIDENCIAL

4. Empleo de datos de carácter personal

Todo usuario que utilice datos de carácter personal para el desempeño de sus funciones ha de conocer que:

- Sólo se pueden utilizar los datos personales para la **finalidad** con la que el afectado los ha entregado. Para ello, los empleados deben conocer la finalidad de la información que manejan y disponer del **consentimiento inequívoco** de la persona para poder tratar sus datos personales.

  Este permiso no es para siempre, puede ser revocado por varios motivos: no cesión a otras entidades, no envío de publicidad (también conocido como Robinson), denegación total del uso de los datos, borrado de los datos de la persona por petición expresa.

- **Cualquier uso diferente** del habitual debe ser previamente **consultado** con el Responsable de Seguridad.

- **No se deben comunicar datos personales** bajo ningún concepto, a no ser que esté explícitamente autorizado y consentido por el afectado.

  Las **cláusulas y contratos** han de reflejar este consentimiento.

- Todos los empleados deben conocer los **derechos** que tiene la persona con respecto a sus datos personales, así como conocer los **procedimientos implantados por NH Hotel Group para atender a estos derechos**.

CONFIDENCIAL

5. Medidas técnicas a aplicar por los usuarios

Todo usuario ha de establecer una serie de medidas que garanticen la seguridad de los equipos y la imposibilidad por parte de terceras personas de acceder a datos de carácter personal. Las medidas a aplicar son:

- Cada usuario accederá a los distintos aplicativos y funcionalidades con su **código de usuario y contraseña**. Se recuerda que el uso de las claves de acceso a los aplicativos es estrictamente personal estando prohibido su uso por cualquier otra persona distinta del titular de la misma.

  El acceso no autorizado a ficheros por parte de los usuarios implica una transgresión de las medidas de seguridad pudiendo producirse sanciones a NH Hotel Group de importante cuantía, por parte de la Agencia de Protección de Datos.

  Las contraseñas no se deben compartir ni anotar en ningún sitio.

- Se han de emplear **contraseñas** que cumplan con los requisitos de robustez y caducidad definidos en el **Anexo V - Control de acceso del Documento de Seguridad del NH HOTEL GROUP**.

- Uso de los equipos de trabajo:
  - **Todo terminal ha de bloquearse** cuando no se esté trabajando, así como tener activado el bloqueo automático de equipos.
  - Se han de seguir las pautas definidas en el **Anexo VI - Gestión de soportes del Documento de Seguridad del NH HOTEL GROUP**.

- Todo **fichero de trabajo** debe almacenarse en carpetas de red con el objetivo de garantizar la realización de copias de seguridad y el acceso controlado al mismo.

- Se ha de evitar guardar **fichero temporales** con información no necesaria o replicada. No **se debe extraer información** a dispositivos portátiles, a **no ser que se esté autorizado** por el responsable correspondiente.

  Una vez **empleada la información** del fichero temporal se deberá **comunicar** al responsable **para proceder a su desechado o almacenamiento** en caso de ser necesario.

- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el correcto desarrollo de sus funciones.

- Las personas que tengan acceso a este tipo de información, o bien reciban información de clientes en cualquier tipo de soporte, tendrán la obligación de cumplir las normas y procedimientos de seguridad y confidencialidad que se establezcan en cada momento.

CONFIDENCIAL

6. Medidas organizativas

La Entidad, así como los usuarios, ha de garantizar las oportunas medidas organizativas que permitan garantizar las medidas de seguridad exigidas por la LOPD y su Reglamento de Desarrollo asociado.

- **Altas/bajas de usuarios**
  - Se debe conocer la Política de Seguridad de la compañía, en el que se recogen los requisitos de gestión de usuarios.
  - Los responsables de cada departamento deben notificar los cambios que les competen, tanto por bajas de usuarios como por cambios en sus funciones.
- **Circuito de la información**
  - Los empleados deben conocer el circuito de la información de carácter personal implantado en NH Hotel Group (al menos la parte que le corresponda):
    - > ¿De quién tengo que recibir la información?
    - > ¿Cómo debo procesar esta información?
    - > ¿A quién puedo comunicar la información?
  - En caso de observar alguna excepción, se debe comunicar inmediatamente al responsable de NH Hotel Group.
- **Gestión de soportes**
  - Cada empleado debe comunicar a su responsable los soportes que tiene, para poder inventariarlo.
  - La creación de soportes ha de estar autorizada por el Responsable de Área del usuario.
  - Toda salida de soportes debe estar autorizada. De igual modo, se han de registrar las entradas y las salidas de los soportes.
  - Se incluye en este documento un capítulo especialmente dedicado a los soportes
- **Gestión de incidencias**
  - Todos los empleados deben conocer el procedimiento de comunicación de las incidencias (ver **Anexo X – Registro de incidencias).**
  - En la medida de lo posible, se debe formar a los usuarios para que la utilización de la

CONFIDENCIAL

aplicación de gestión de incidencias sea eficaz. La definición de "incidencia" sea consistente en toda la organización y sea conocida por todo el personal.

6.1 Gestión de soportes

Los soportes (cintas, discos, CD's, papel, etc.), que contengan datos de carácter personal, deberán estar perfectamente inventariados así como almacenados en un lugar con acceso restringido al personal autorizado.

El tratamiento a seguir en el caso en que se reciban soportes de otras empresas que contengan datos de carácter personal, deberá adecuarse a las normas indicadas en este apartado, hasta que se produzca la devolución del soporte a dicha empresa.

Los ficheros deben utilizarse para la finalidad para la que fueron creados, por lo que no se podrán utilizar con otros fines.

La salida de soportes que contengan datos de carácter personal, fuera del local en el que se ubica el fichero, deberá ser autorizada por el Responsable de Tratamiento del Fichero.

El uso de la información facilitada a través de transferencias de ficheros – file transfer – deberá ser el de la finalidad para la que los ficheros iniciales se crearon. En el caso de que su tratamiento diera lugar a nuevos ficheros diferentes en su finalidad a la de origen, deberá ser comunicado a Asesoría Jurídica para su incorporación en la declaración ante la AEPD.

En las prestaciones de servicios de terceros, deberá garantizarse la correcta utilización de los mismos siendo necesario cumplir los siguientes requisitos:

- Autorización por parte del Responsable de Tratamiento del Fichero, para la salida de datos fuera de los locales dónde se ubica el fichero.
- Asesoría Jurídica firmará un contrato con la persona receptora de la información con las cláusulas de confidencialidad necesarias, por el que se le compromete a utilizar la información de acuerdo con la finalidad para la que se ceden y a establecer las medidas de seguridad correspondientes al nivel de seguridad declarado en la Agencia de Protección de Datos.
- Además se dejara constancia en el contrato de la posibilidad de realizar una auditoría por parte del encargado del tratamiento para verificar la correcta utilización de la información.

6.2 Copias de respaldo y recuperación

Los procedimientos existentes para la realización de copias de respaldo y recuperación de datos, deben garantizar la reconstrucción de los mismos en el estado en que se encontraban en el momento en que se produjo la pérdida o destrucción.

Deberán realizarse copias de seguridad al menos semanalmente, salvo cuando en ese periodo no se hubiera producido ninguna actualización de datos.

CONFIDENCIAL

En el caso de ficheros cuya información resida en el ordenador central, las copias de respaldo las realizará el Departamento de Tecnologías de la Información. En los casos excepcionales de ficheros diferentes a los anteriores y que estén declarados a la Agencia de Protección de Datos, este procedimiento se llevará a cabo por el administrador del fichero que previamente se haya nombrado al efecto.

6.3 Gestión de incidencias

Se ha establecido un circuito que afectará a todas las unidades del NH Hotel Group para la canalización y resolución de incidencias que se puedan producir. Dentro de estas incidencias se considera cualquier anomalía que pudiera afectar a la seguridad de los datos de carácter personal: incumplimiento de las normas descritas, acceso a ficheros no autorizados, cesión de la contraseña, salida de información sin previa autorización o cualquier otra incidencia que a su criterio pudiera vulnerar la normativa de seguridad. Para más información, ver **Anexo X – Registro de incidencias**.

CONFIDENCIAL

7. Medidas relativas al papel

El Reglamento de Desarrollo de la LOPD especifica una serie de medidas a aplicar en la seguridad de los datos personales en ficheros no automatizados, donde se incluye el tratamiento del papel. Dentro de las medidas de seguridad, el usuario ha de conocer los siguientes aspectos:

- **Inventario y clasificación**
  - Se debe conocer la clasificación de la información definida en NH Hotel Group, así como el **procedimiento de etiquetado** que se haya establecido.
  - Todos los empleados deben colaborar en mantener un inventario actualizado del papel, comunicando los cambios al responsable designado.
  - Toda la información se ha de almacenar en el archivo asignado.
  - En caso de ser necesario sacar un documento del archivo, cada empleado es responsable de mantener la confidencialidad de dicho documento hasta que sea devuelto.
- **Mesas limpias**
  - Se debe limitar número de papeles de trabajo que los empleados tienen fuera del archivo.
  - Una posibilidad es mantener cajones con llave en los puestos de trabajo.
  - Una vez se finalice de trabajar con un documento, habrá que:
    - > Devolverlo al archivo si es el documento original.
    - > Destruirlo si es una copia o fichero temporal.
  - Al finalizar la jornada de trabajo, las mesas han de permanecer libres de papeles y/o cualquier otra documentación sensible.
- **Destrucción de papel**
  - Toda información de carácter personal que se quiera desechar debe ir a los depósitos habilitados a tal efecto.
  - Los contenedores deben cumplir con las medidas exigibles.

CONFIDENCIAL

8. Medidas de seguridad en los equipos de comunicación de usuarios

- **Uso de FAX**
  - Se debe evitar enviar faxes a terminales públicos.
  - Si se espera recibir algún fax, se debe estar presente para evitar que lo recoja otra persona.
- **Uso impresoras**
  - En caso de imprimir algún documento, el usuario debe recogerlo inmediatamente si no existe control de acceso.
- **Uso fotocopiadoras**
  - En la medida de lo posible, se debe evitar su uso ya que implica replicar información.
  - En caso de copias documentos, las copias se deben destruir cuando no sean necesarias (fichero temporal, destrucción de documentos).
- **Correo electrónico**
  - Se debe solicitar autorización para enviar datos de nivel alto por correo electrónico.

CONFIDENCIAL

9. Recursos de NH Hotel Group. Para la Divulgación Y Concienciación.

Como parte del procedimiento difusión y concienciación de la LOPD, se están empezando a desarrollar acciones para tal fin. Destacan:

- Curso de Concienciación y Divulgación.
- Publicación en intranet (ver **A01.1 - Resumen LOPD Portal NH Hotel Group (procedimiento)** y **A01.3 - Ley Orgánica Protección Datos FAQs)**.
- Sección Compliance en la intranet (http://employeeportal.nh-hotels.com/portal/page/portal/EmployeePortal/COUNTRY_CORPORATIVE/EMPLOYEEAREANEW/COMPLIANCE/Menu_Compliance/CRIMINAL%20RISK%20PREVENTION/LEGISLATION%20MENU/Personal%20Data%20Privacy)
- Documentación de bienvenida.
- Envíos periódicos de correos de sensibilización (ver documento **A01.2 - Email de concienciación LOPD (procedimiento)**).

Todos los recursos anteriormente descritos pueden ser usados para su publicación en la Intranet, así como su distribución en trípticos, correo electrónico u otros medios. Los recursos se encuentran en formato genérico y se irán personalizando según las situaciones.

CONFIDENCIAL