nH | HOTEL GROUP

Normativa sobre protección de datos de carácter personal

La Información

• Es un activo muy importante para NH Hotel Group: no debes disponer de ella a tu antojo.

• Eres el responsable de la información que manejas, en cuanto a su difusión, utilización, mantenimiento, etc.

• La L.O.P.D. penaliza el uso indebido y la posesión injustificada de datos personales.

• La información confidencial no está sólo en el ordenador, ten cuidado con el papel u otro soporte (pen drives, CD ROM, etc.).

• Cuando crees ficheros que contengan datos personales para uso temporal recuerda que tendrás que borrarlos cuando no los necesites. En el caso de tratarse de ficheros en formato papel deberá utilizarse las destructoras habilitadas para tal efecto

• No emplees ficheros que puedan contener datos de carácter personal desactualizados, solicita siempre la copia más actual posible.

• Evita la utilización del correo electrónico externo para el envío de datos de carácter personal.

Las normas de seguridad se han creado para facilitar tu trabajo, garantizar la seguridad de la información de NH Hotel Group y el cumplimiento de la ley

Unas nociones básicas acerca de la LOPD

• La LOPD surge a partir del art. 18 de la Constitución, con el objetivo de reforzar la protección de la intimidad de las personas físicas, en lo relativo al tratamiento de sus datos personales.

• Esta Ley se aplica a los datos de carácter personal registrados en soporte físico, que los haga susceptible de tratamiento, y a toda modalidad de uso posterior de estos datos.

• Dato de carácter personal es, a estos efectos, cualquier información concerniente a personas físicas identificadas o identificables.

• Dentro del concepto Tratamiento de datos se comprenden las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias. Vemos, por tanto, que se trata de un concepto muy amplio que abarca prácticamente cualquier operación que realices sobre los datos de carácter personal.

• Derivado de la LOPD aparece la figura de Responsable de Seguridad que se encarga de elaborar, coordinar y controlar las medidas de seguridad aplicables. Actualmente, esta responsabilidad recae sobre el Director de Tecnologías de la Información de NH Hotel Group.

Copias de seguridad y soportes

• Haz copias de seguridad siguiendo las normas establecidas. Es la mejor forma de asegurar la disponibilidad de tus datos.

• Haz copias de seguridad de tus ficheros cuando los modifiques.

• Recuerda siempre que para que se puedan realizar copias de seguridad de forma automática y segura, deberás almacenar tus archivos en el servidor.

• Si haces alguna copia de seguridad en soporte magnético, guárdalo en un lugar seguro cuando acabes tu trabajo diario, de forma que impidas que puedan ser robados o alterados. No los dejes encima de la mesa cuando termines. Etiquétalos de forma que identifiques el contenido y la fecha de los mismos.

• Asegúrate de la existencia de una autorización del Responsable del Fichero antes de sacar un soporte o un equipo portátil con datos de carácter personal fuera de su ubicación habitual.

Ten en cuenta la normativa existente respecto a la entrada y salida de soportes con datos de carácter personal.

¿Qué es la L.O.P.D.?

- La L.O.P.D. es la Ley Orgánica 15/1999 de diciembre de Protección de Datos de Carácter Personal publicada en el BOE el lunes 13 de Diciembre de 1999, teniendo 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 su honor e intimidad personal y familiar.

- El día 26 de junio de 1999, entró en vigor el Real Decreto 994/1999 por el cual quedaba aprobado el Reglamento de Medidas de Seguridad de los Ficheros Automatizados de Datos de Carácter Personal. En dicho reglamento se establecen las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal.

- El Real Decreto 1720/2007, de 21 de diciembre, aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Este Real Decreto 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. Comprende por tanto el tratamiento automatizado y el no automatizado de los datos de carácter personal.

- Con la aparición del Reglamento de Medidas de Seguridad NH Hotel Group ha adaptado a dicho Reglamento sus actuales medidas de seguridad organizativas y técnicas sobre los ficheros declarados a la Agencia de Protección de Datos y así cumplir con los preceptos establecidos en la L.O.P.D. y en Real Decreto 994/1999.

Evolución de la Normativa y el Reglamento de Medidas de Seguridad

1992	Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.
1993	Real Decreto 428/1993, de 26 de junio, Estatuto de la Agencia de Protección de Datos.
1994	Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992 de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.
1995	Instrucción 1/1995, de 1 de marzo, de la APD, relativa a la prestación de servicios de información sobre solvencia patrimonial y crédito.
1998	Instrucción 1/1998, de 19 de enero, de la APD, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
1999	Real Decreto 994/1999, del 11 de junio de 1999, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.
1999	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
2000	Instrucción 1/2000, de 1 de diciembre, de la APD, relativa a las normas por las que se rigen los movimientos internacionales de datos.
2007	Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Contraseñas

- Utiliza una contraseña de entrada al ordenador para impedir el acceso a tus datos y a las aplicaciones.
- Tú eres el responsable de la confidencialidad de tu contraseña.
- Utiliza contraseñas de al menos 8 caracteres y que sean alfanuméricas, siempre que lo admita el sistema.
- No utilices una contraseña que sea igual que tu identificador, nombre, apellido, fecha de nacimiento, etc.
- No la anotes en lugares visibles ni la compartas con los demás.
- Cambia de contraseña la primera vez que accedas al sistema y periódicamente cada 90 días.

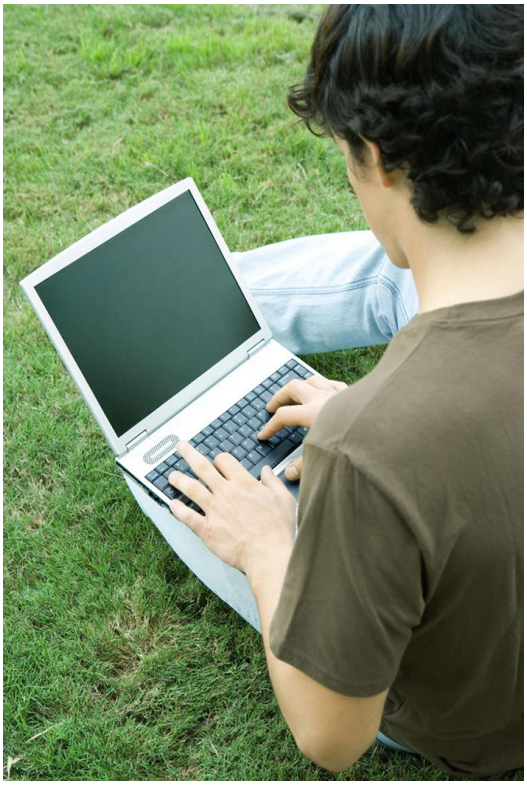
- Bloquea tu ordenador con las teclas CTRL ALT SUPR (pulsando las tres a la vez) para cuando dejes de trabajar con el ordenador de forma momentánea.

Otros aspectos de interés

- Antes de enviar la información mediantes redes de telecomunicaciones, es necesario cifrarla.

- Si eres responsable de ficheros con datos de carácter personal, deberás velar por la integridad y confidencialidad de los documentos, siempre que no se encuentren archivados por estar en proceso de revisión o tramitación.

- Realiza sólo copias si tienes la autorización del responsable. Si se trata de documentación de carácter personal de nivel alto, evita realizarlas.



Derechos y obligaciones

Tus derechos

• Tienes derecho a utilizar la información del modo que sea necesario para el cumplimiento de tus responsabilidades de trabajo.

• Así mismo, tienes derecho a conocer las normas de seguridad que afecten al desarrollo de tus funciones.

• Durante el desarrollo normal de tu trabajo, el personal de sistemas únicamente accederá a tu equipo en caso de incidencia técnica y previa autorización por tu parte.

Tus responsabilidades y obligaciones

• Debes respetar las normas establecidas con respecto a la seguridad de los sistemas informáticos y la información que en ellos se trata.

• Eres responsable de utilizar los mecanismos y procedimientos disponibles para la protección de tus datos, así como los datos que se hallan bajo tu control.

• Cualquier incumplimiento de esta normativa tiene consecuencias legales.

¿Qué obligaciones debo cumplir en el tratamiento de datos de carácter personal?

• Si creas un fichero con datos de carácter personal que incluya campos de datos o que tenga fines distintos de los que utilizas habitualmente, deberás comunicarlo al Responsable de Seguridad, a los efectos de mantener actualizadas las declaraciones a la Agencia de Protección de Datos.

• Si efectúas una recogida de datos por una vía distinta a las habituales, recuerda la necesidad de utilizar procedimientos por los que se obtenga el consentimiento informado del interesado.

• Los datos personales que revelen ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual tienen la consideración de especialmente protegidos, y exigen cuidados especiales.

• El principio de calidad de los datos nos obliga a que sólo podamos utilizar los datos personales necesarios en relación con la labor que estemos realizando.

• Debes guardar secreto profesional y confidencialidad con respecto a los datos personales a los que accedas por razón de tu puesto de trabajo.

• Los interesados tienen derecho a acceder, rectificar, cancelar y oponerse al tratamiento de sus datos personales. Si recibes alguna incidencia de este tipo, ponte en contacto, inmediatamente, con el Responsable de Seguridad, hay un plazo límite de tiempo para gestionarlo.

• No comuniques datos personales a terceros sin adoptar las medidas necesarias, ya que se requiere el consentimiento del interesado o bien incluir una cláusula especifica en el contrato que regule la relación con el destinatario de los datos.

• Debes notificar cualquier incidencia de seguridad que se produzca sobre la información o los sistemas con los que trabajes habitualmente que pueda comprometer datos de carácter personal al Responsable de Seguridad. Esta recomendación es extensible a la información en formato papel, para la que también existe un registro de incidencias.

Qué debo hacer y qué no debo hacer

¿Pero qué debo hacer?

… te estarás preguntando.

Te mostramos una pequeña serie de cosas que puedes hacer para colaborar:

• Las contraseñas son la mejor forma de impedir que alguien acceda a tus datos. **¡Utilízalas!**. Cámbialas periódicamente.

• Si detectas que alguien ha accedido a tu usuario o conoce tu contraseña, comunícalo a HELP-DESK; están para ayudar.

¿Y qué no debo hacer?

Y aquí están algunas de las cosas que no debes hacer:

• Comunicar a otros tu contraseña de acceso.

• Permitir el uso de tu ordenador a personas no autorizadas.

• Usar la información irresponsablemente transmitiéndola o facilitando el acceso a personas ajenas a tu trabajo.

• Si tienes dudas sobre una determinada conducta en relación con el uso de datos personales, no actúes, pregunta al Responsable de Seguridad.