

> MANUAL USUARIO PARA LA PROTECCIÓN DE INFORMACIÓN CORPORATIVA. RESPONSABILIDADES

Documento:

Versión	Fecha	Autor:	Revisado:	Aprobado:
1.0	DIC-13	Jaime Velasco		
2.0	ENE-15	Jaime Velasco		

Control de Cambios:

Versión	Fecha	Modificaciones
2,0	ENE-15	Adaptación a requerimientos CD

Clasificación:

Propietario	Nivel		
Responsable Seguridad Información	☐ Confidencial	☒ Uso Interno	☐ Público

Contenidos:

1. OBJETIVO	3
Introducción.....	3
2. ALCANCE	4
3. ¿QUÉ ES SEGURIDAD DE LA INFORMACIÓN Y POR QUÉ AFECTA A NH?	5
4. QUE TIPOS DE INFORMACIÓN SE HAN DEFINIDO EN NH?	6
5. CONTROL DE ACCESO	10
6. PROTECCION FRENTE A SOFTWARE MALICIOSO	12
7. SEGURIDAD DE LOS SERVICIOS DE RED DE NH	13
8. UTILIZACION DEL CORREO ELECTRÓNICO	15
9. EQUIPOS Y SOFTWARE.....	16
10. COMUNICACIÓN DE INCIDENCIAS DE SEGURIDAD	18
11. TRATAMIENTO DE DATOS DE SENSIBLES	19
12. REVISION.....	20
13. Y RECUERDA QUE.....	21

1. OBJETIVO

Introducción

El objeto del presente documento es el de proporcionar al personal propio, ajeno o en prácticas que acceda a Información de NH Hotel Group (a partir de ahora NH), un conjunto de directrices y pautas de comportamiento necesarias para garantizar la seguridad de la misma.

Dichas directrices constituirán las responsabilidades a asumir por el personal en el desarrollo de su actividad laboral en NH, con objeto de proteger la Información corporativa, y asegurar que su uso es adecuado, responsable y lícito de los activos de información.

2. ALCANCE

El alcance del presente documento incluye a todos los empleados de NH incluyendo al personal externo o en prácticas, con acceso a información de NH.

Se entiende por información de NH, toda aquella generada, transformada, almacenada o eliminada por los empleados, personal externo y personal en prácticas que trabajen para NH, en el desarrollo de los procesos de negocio y de soporte corporativos, incluida aquella sobre la que se tienen derechos de propiedad intelectual, así como la cedida por terceros y sobre la que NH actúa como agente tratante.

NH pone a disposición de sus usuarios la capacidad de acceder a los sistemas de información y visualizar o modificar la información que procesan y almacenan. Los permisos de acceso a las redes, sistemas y a la propia información serán otorgados mediante un proceso formal de aprobación que asegure que los usuarios tengan acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones.

Como premisa general, todo usuario está obligado a utilizar los equipos y sistemas de información puestos a su disposición sin incurrir en actividades ilícitas, ilegales o que pongan en riesgo la seguridad de la información alojada en los sistemas de información.

La utilización de los activos informáticos se fundamenta en los siguientes principios generales:

- El uso de los activos de información está vinculado exclusivamente al cumplimiento del desempeño de las funciones de negocio.
- El usuario no comunicará a personas no autorizadas o al exterior de NH información restringida, por ningún medio o soporte, salvo previa autorización por parte del responsable de la información.
- Los responsables de la información deberán definir qué información puede ser tratada mediante dispositivos portátiles, teniendo que estar accesibles únicamente para el personal autorizado.
- Los usuarios de los sistemas de información, deberán respetar los derechos del resto de usuarios y demostrar, en el uso de estos recursos y servicios, el mismo respeto que normalmente se tiene en las comunicaciones verbales.
- El tratamiento de la información desde su creación hasta su almacenamiento, deberá de realizarse de forma que asegure su disponibilidad, integridad y confidencialidad.

3. ¿QUÉ ES SEGURIDAD DE LA INFORMACIÓN Y POR QUÉ AFECTA A NH?

De manera constante se está produciendo un desarrollo tecnológico en la manera que trabajamos, esto se traduce en la implantación de aplicaciones e infraestructura informática destinada a agilizar y optimizar nuestra operativa de trabajo, ayudándonos a realizar nuestras funciones y haciendo que nuestra compañía sea más competitiva, aumentando la calidad del servicio ofrecido al cliente.

Cambia la manera como los empleados podemos acceder y tratar la información de NH, ya sea desde nuestras oficinas, hoteles o en remoto desde cualquier lugar, también cambia la manera como nos relacionamos con terceros, facilitando la conexión de otras empresas que necesitamos para desarrollar nuestro negocio y por supuesto cambia la manera como nuestros clientes pueden relacionarse con nuestros sistemas para poder gestionar sus requerimientos.

Todo lo anterior ha provocado la aparición de nuevas formas de acceder, utilizar, almacenar y eliminar la Información de NH. Pese a que lo que se ha hecho tiene un gran número de ventajas, también provoca la aparición de nuevas responsabilidades para todos. Tenemos que proteger la Información de la compañía frente a tres riesgos fundamentales:

- que sea accedida o divulgada, sin autorización, por terceros,
- que no esté disponible cuando la necesitemos para realizar nuestro trabajo,
- y que ésta no sea integra.

Todos debemos ser conscientes de que la información es uno de los principales activos corporativos, y que si se ve comprometida puede provocar graves daños a la posición competitiva y a la imagen de NH, y por extensión, a la nuestra, como empleados o colaboradores que somos. Por tanto, todos debemos, en la medida de nuestras posibilidades y según nuestra posición, garantizar la Seguridad de la Información de NH.

La Seguridad de la Información de NH es una responsabilidad compartida que requiere el compromiso de todos y cada uno de sus empleados, personal externo y en prácticas.

- Necesitamos que seas muy cuidadoso con la Información de NH que utilizas en tu trabajo y que cumplas tus responsabilidades en materia de Seguridad de la Información.
- Si tienes dudas, pregunta al Área de Seguridad de la Información. ¡Estaremos encantados de ayudarte! Para ello puedes dirigirte a la cuenta de correo infosec@nh-hotels.com

4. QUE TIPOS DE INFORMACIÓN SE HAN DEFINIDO EN NH?

Con objeto de proteger adecuadamente la información de NH, se han definido una serie de categorías para clasificar la misma en función de su importancia. Estas categorías son las siguientes:

- **Confidencial:** Es la información más importante. Su divulgación o acceso no autorizado tendría un impacto muy grande para la compañía, para sus empleados, para sus accionistas y para sus clientes. Entre este tipo de Información están tus datos económicos (incluyendo los de tu evaluación) y médicos, los datos sensibles de los clientes y accionistas, los planes estratégicos de la compañía (como grupo), tus contraseñas de acceso a las aplicaciones de NH, los resultados de los procesos de selección de nuevos empleados, etc. Si tienes acceso a Información de este tipo, debes ser especialmente cuidadoso.
- **Difusión Limitada:** Es información importante, pero no tan sensible como la Confidencial. Está destinada a ser compartida por un conjunto de personas, en función de su cargo o función. Entre este tipo de Información se encuentran tus datos personales, los datos generales de los clientes, los presupuestos departamentales, los datos de los diferentes proveedores, los datos económicos y financieros de las diferentes sociedades del Grupo, y en general, toda la Información que deba ser conocida por un departamento/área o grupo de actividad. Debes tener en cuenta que si la Información no tiene clasificación, deberás tratarla como si fuese de Difusión Limitada.
- **Uso Interno:** Es información destinada a todo el personal de NH, independientemente de su actividad o función. Incluye, datos profesionales de los empleados, boletines y circulares internas, noticias publicadas en la Intranet, información divulgativa para todos los empleados y políticas y procedimientos que deban estar accesibles para todos los empleados.
- **Pública:** Información destinada a ser divulgada al público general y que, por tanto, no necesita protección.

La Información necesita una protección diferente según su clasificación. Ten siempre presente qué tipo de Información manejas y actúa en consecuencia

- Tienes unas responsabilidades generales y otras que dependen del tipo de Información.
- Toda Información tiene asociado un Propietario, que es el responsable de garantizar su Seguridad. En general, será la persona que genere esa Información, la encargada de clasificarla acorde a los criterios vistos. Si tienes dudas, pregunta al Área de Seguridad de la Información.

Toda comunicación pública de información de NH deberá ser revisada y aprobada por el Departamento de Comunicación

- No comentes información de NH a los medios de comunicación, independientemente de las circunstancias que puedan darse. Este tipo de comunicaciones debes remitirlas al departamento de Comunicación.
- Si necesitas divulgar, interna o externamente, información clasificada como de Difusión Limitada o Confidencial, solicita previamente al Propietario su aprobación.

No generes, almacenes o proceses información de NH en equipos que no pertenezcan a la compañía

- Si necesitas tratar información de NH en tu equipo particular, pide permiso al Responsable de Seguridad.
- No accedas a Información Confidencial de NH desde equipos situados en lugares públicos y sobre los que NH no tenga ningún tipo de control.

No indiques la clasificación de la información en las propiedades del documento, sobres o envoltorios externos cuando la envíes al exterior

- Comprueba que se cumple la siguiente regla: sólo después de acceder directamente a la Información es posible conocer su nivel de sensibilidad.
- Cuando necesites enviar Información Confidencial, asegúrate de que para el transporte de los soportes de almacenamiento (o documentos) se utiliza un sobre o recipiente sellado.

No dejes accesibles a cualquiera papeles o soportes que contengan información de Difusión Limitada o Confidencial

- Mantén tu mesa y armarios ordenados, guardando los documentos, y cualquier soporte digital de información en cajones cerrados.
- No dejes a la vista papeles con Información de Difusión Limitada o Confidencial.
- Cuando recibas soportes con Información de Difusión Limitada o Confidencial, en la medida de lo posible comunica un acuse de recibo (por teléfono o e-mail).

Garantiza la seguridad de la Información cuando reutilices o destruyas documentos o soportes

- No reutilices como borrador papeles que puedan contener Información de Difusión Limitada o Confidencial.
- Borra los soportes que hayan contenido Información de Difusión Limitada o Confidencial antes de regrabar sobre ellos.
- No almacenes información de menor nivel de sensibilidad en soportes que hayan contenido Información Confidencial o de Difusión Limitada, siempre que vayan a ser utilizados por personas diferentes.
- Utiliza las trituradoras para destruir Información de Difusión Limitada (o de sensibilidad superior) en soporte papel. Rompe los documentos con información de NH antes de depositarlos para que sean reciclados.

No tengas conversaciones telefónicas en lugares públicos, o dejes mensajes de voz, en los que trates información sensible de NH

- No dejes mensajes relativos a Información de Difusión Limitada o Confidencial en buzones de voz de personas ajenas a NH.
- Evita las conversaciones en lugares públicos, o utilizando sistemas de altavoz y manos libres, que versen sobre Información Confidencial.

No envíes por fax información Confidencial

- Si es imprescindible utilizar el fax, verifica la identidad del receptor y el número de teléfono proporcionado y solicita acuse de recibo, por teléfono o mediante correo electrónico.

Protege tu equipo cuando no estés presente

- Si abandonas momentáneamente tu puesto de trabajo, bloquea tu equipo, pulsando las teclas Ctrl+Alt+Supr y escoge la opción “Bloquear equipo”.
- Cuando finalices tu jornada laboral, apaga tu equipo.

No realices copias de información de Difusión Limitada o Confidencial sin el consentimiento del Propietario

- Si haces copias temporales (por ejemplo, cuando imprimas un documento que tienes en formato electrónico), protégelas en función de su clasificación. Cuando dejes de utilizarlas, elimínalas, utilizando los mecanismos puestos a tu disposición.
- No envíes ni saques de las instalaciones de NH información corporativa sin la autorización expresa del propietario. Si es Información Confidencial, debes garantizar además que la misma se encuentra cifrada en el soporte utilizado para su transporte y almacenamiento.

No abandones en la bandeja de la impresora documentos que incluyan información de Difusión Limitada o Confidencial

- Si no se dispone de algún medio de control adicional en las impresoras, acude inmediatamente a la impresora para recoger los documentos.
- Imprime la información de carácter Confidencial en impresoras personales o situadas en áreas controladas.

No almacenes información Confidencial en la carpeta del Departamento

- Almacena la información Confidencial que manejes en tu trabajo en tu carpeta personal.
- Almacena la información de Difusión Limitada en la carpeta departamental sólo si todas las personas del departamento están autorizadas para acceder a la misma.

Sólo tú puedes proteger la Información que utilizas en el desarrollo de tu trabajo. NH te proporcionará los mecanismos y la formación que necesitas para hacerlo

5. CONTROL DE ACCESO

Acceso

- A cada usuario se le permitirá el acceso sólo a aquellos recursos, unidades de red y carpetas que requiera para el correcto desempeño de sus funciones de negocio, denegándose los restantes accesos.
- Se deshabilitarán aquellos dispositivos que se estime no sean necesarios para el desarrollo del trabajo del usuario y puedan hacer peligrar la confidencialidad e integridad de la información tratada en el PC.

Deber de secreto

- El propietario de la información y quienes intervengan en cualquier fase del tratamiento información restringida, están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones laborales o contractuales con NH o con el departamento al que pertenece. Estas obligaciones consideradas en los contratos o acuerdos de los empleados, podrán incurrir en acciones legales en el incumplimiento de las mismas, según dicta la legislación vigente.

No divulgues tus contraseñas de acceso

- Si por causas justificadas necesitas comunicar a alguien tu contraseña, pide permiso a tu Responsable y cámbiala inmediatamente después de que haya sido utilizada.
- No anotes tus contraseñas en papeles a la vista.
- Evita introducir tu contraseña de acceso cuando estés siendo observado de cerca por terceros que no tengan acceso a la Información que manejas.
- No accedas a sistemas o aplicaciones de NH utilizando el usuario y contraseña de otra persona.
- Si utilizas un usuario compartido, comprueba que se cambia la contraseña cuando cambien los usuarios que la utilizan.

Utiliza contraseñas de calidad y cámbialas periódicamente

- Utiliza contraseñas de al menos seis caracteres de longitud, que incluyan caracteres alfanuméricos (mayúsculas y minúsculas) numéricos
- No utilices palabras “comunes” a la hora de generar tus contraseñas. En general, evita utilizar palabras que puedan aparecer en diccionarios.
- No utilices información personal que pueda conocerse fácilmente (p.e: fecha de nacimiento, etc.) cuando generes tu contraseña. Tampoco uses secuencias numéricas, alfanuméricas o de letras del teclado fácilmente adivinables (p.e: 12345678, asdfghjk, abcd1234, contraseña, etc.).
- Cuando cambies tu contraseña, evita el uso “contadores” (por ejemplo, contraseña antigua: nh_central1; contraseña nueva: nh_central2).

Ten siempre presente que eres responsable de las acciones realizadas con tu usuario personal en las aplicaciones y Sistemas de Información de NH

- Si sospechas que alguien puede estar utilizando tu usuario de forma no autorizada, comunícalo inmediatamente con el área de Seguridad de la información.

6. PROTECCION FRENTE A SOFTWARE MALICIOSO

No instales en tu equipo aplicaciones que no hayan sido homologadas por NH

- No instales software copiado ilegalmente o del que no tengas licencia.
- No instales software de uso personal en equipos de NH.

Si sospechas que tu equipo está infectado, ponte en contacto con el Área de Seguridad de la Información

- Notifica al Área de Seguridad de la Información la recepción de cualquier correo electrónico no solicitado o de contenido sospechoso.
- Si te envían un correo que no has solicitado, o que encuentras sospechoso no abras el contenido adjunto y elimínalo.

No conectes a tu equipo dispositivos externos no homologados por NH

- Ten especial cuidado cuando conectes memorias USB o discos duros portátiles a los equipos pertenecientes a NH.
- No conectes dispositivos de grabación, cámaras digitales, agendas electrónicas personales, reproductores musicales, etc., en los equipos propiedad de NH, que no hayan sido homologados.
- No copies información personal, o que no esté relacionada con tu trabajo, en equipos de NH.

No desactives el antivirus instalado en tu equipo

- No interrumpas su ejecución. Si en ese momento te impide la realización de un trabajo urgente, posponlo, pero nunca lo pares.
- Si el antivirus interfiere con la ejecución de otros programas, informa al área de Seguridad para que analice el problema.
- Si no te conectas habitualmente a la red de NH, pregunta al Área de Sistemas cómo actualizar tu antivirus manualmente.

7. SEGURIDAD DE LOS SERVICIOS DE RED DE NH

Guarda en tu carpeta personal la información importante que manejes y de la que quieras tener copia de seguridad

- Evita almacenar en esta carpeta información que no sea resultado de tu actividad laboral o que no sea relevante

Haz un uso profesional y racional del servicio de acceso a Internet corporativo, evitando acceder a sitios con contenido inadecuado o peligroso

- No accedas a páginas de contenido violento, ofensivo para personas, colectivos o empresas, pornográfico, destinado a establecer redes P2P, o que incluya métodos y herramientas destinadas a “piratear” servicios y programas comerciales. Estas páginas son muy peligrosas, ya que suelen instalar software malicioso (malware) en los equipos de los usuarios, poniendo en peligro la seguridad de la Información corporativa.
- No utilices servicios de navegación anónima. En NH ya hemos establecido mecanismos destinados a garantizar la privacidad de tu navegación.
- No utilices programas destinados a burlar las normas anteriores. Estarías comprometiendo la Seguridad de la Información de NH.

No conectes dispositivos de conexión a Internet sin la autorización expresa

- Sólo los equipos autorizados podrán hacer uso de dispositivos de conexión a Internet

Protege tu ordenador portátil y dispositivos externos, especialmente cuando estés fuera de las instalaciones de NH

- Si lo vas a dejar momentáneamente desatendido, guárdalo en un sitio seguro (cerrado con llave) o átaló (en el caso de portátiles) utilizando los candados proporcionados por el Área de Sistemas.
- Para prevenir “infecciones” por software malicioso, evita utilizar equipos que no sean propiedad de NH para acceder remotamente a la Red Corporativa.
- Si vas a viajar con tu equipo, no lo factures. Llévalo siempre contigo como equipaje de mano.
- En caso de robo, ponte inmediatamente en contacto con el área de Seguridad de la Información

Mesa limpia y protector de pantalla

- Los sistemas de información, el material informático y los soportes de información, deberán ser cuidadosamente custodiados, adoptando sobre ellos los controles necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información. Estas acciones se deberán de llevar a cabo incluso al término de la jornada laboral.
- Todos los ordenadores de NH o dependientes de este, se configuran inicialmente con un protector de pantalla que exige una contraseña al tiempo de inactividad del mismo, pasado este tiempo, el usuario deberá de introducir de nuevo su contraseña para desbloquearlos, en algunos casos debido a operativa de negocio, esta media de

8. UTILIZACION DEL CORREO ELECTRÓNICO

No uses el correo electrónico corporativo para fines distintos a los estrictamente profesionales

- Sé respetuoso y ético en los mensajes que envíes utilizando tu cuenta corporativa, no envíes mensajes ofensivos para personas, colectivos o empresas, así como aquellos que incluyan contenidos violentos, eróticos, pornográficos, publicitarios o “mensajes en cadena”.
- Si recibes mensajes de las características anteriores procedentes de empleados, colaboradores o personal en prácticas de NH, y observas reincidencia en este comportamiento, comunícaselo al área de Seguridad.
- Cuando renvíes un correo electrónico, asegúrate de copiar siempre al remitente del mismo. Salvo que cuentes con autorización, no utilices la cuenta de correo de otra persona.
- Marca como importante sólo aquellos correos que realmente lo sean.
- Firma con tus datos (nombre, cargo y datos de contacto) todos los correos nuevos que envíes.
- Si vas a realizar una comunicación masiva, solicita la aprobación previa al Responsable de tu Departamento.
- Realiza el mantenimiento periódico de tu cuenta de correo, eliminando o archivando los mensajes con objeto de no superar la capacidad de tu buzón
- Si recibes por error información destinada a otra persona, debes eliminar el correo electrónico sin guardar copia alguna del mismo o de la información adjunta, informando de ello al remitente.

No envíes Información Confidencial sin cifrar, ya que puedes estar comprometiéndola

- Cifra la Información Confidencial antes de enviarla. Si tienes dudas sobre cómo llevar a cabo esta operación, consulta con el Área de Seguridad de la Información

Tus correos pueden ser monitorizados si se sospecha que no cumples con las responsabilidades anteriores

9. EQUIPOS Y SOFTWARE

El puesto de trabajo asignado a cada trabajador de NH se considerará una herramienta de trabajo, y como tal, solo podrá ser utilizado con los fines para los cuales ha sido proporcionado, por ello su uso, deberá regirse por las directrices estipuladas en la política de seguridad de la información.

Bajo ningún concepto, los sistemas de información se deberán de utilizar para:

- La realización de acciones diferentes a las asignadas para la correcta culminación de las funciones de negocio.
- Transmitir información de NH sin la adopción de las salvaguardas que garantizan la confidencialidad de la información.
- Acceder o utilizar la cuenta de otro usuario sin su autorización.
- Suplantar o intentar suplantar, a un usuario a través de la utilización de medios técnicos.

Adquisición de equipos y software

- Los recursos puestos a disposición del usuario son propiedad de NH, por lo que su adquisición seguirá los procedimientos de compra de bienes vigentes en la organización, siendo NH los encargados de la planificación y adquisición, logrando una estandarización general de todos los componentes de hardware y una optimización de los costes de adquisición.
- Consideramos como equipos, al conjunto de elementos físicos o materiales que componen un sistema de información, tales como ordenadores, impresoras, monitores, etc.
- Los usuarios no podrán realizar ningún tipo de cambio, manipulación, modificación o realización de intercambio de dispositivos o componentes hardware entre los sistemas, si no cuentan con la autorización y coordinación sobre todos los procesos de instalación del Departamento de IT & Organización
- El correcto funcionamiento de los equipos depende de la realización de un mantenimiento periódico, proporcionando de esta manera mayor seguridad y un mayor rendimiento a las máquinas.
- Se deberá apagar, al término de la jornada laboral, de forma completa el/los equipos personales, (CPU + Monitor + Periféricos) con el fin de ahorrar energía y alargar la vida útil de los mismos.
- Los equipos llevarán instaladas el software necesario para facilitar el correcto desempeño de las funciones de negocio de los usuarios a los que se destinan.

- Las instalaciones de nuevo software deberán proponerse motivadamente y aprobarse por el Departamento de IT & Servicios Generales.
- El Departamento de IT & Organización dará soporte sobre las acciones de mantenimiento a realizar por el usuario nombradas anteriormente, para cualquier otro tipo de mantenimiento, deberá ser consultado y aprobado por dicho departamento.
- El usuario se compromete a no instalar, sin previa autorización del departamento de IT & Servicios Generales, cualquier programa o aplicación informática distinta a las facilitadas por la organización.
- La utilización de software sin licencia es una conducta ilícita que puede implicar graves responsabilidades de tipo penal y civil, además de poner en riesgo evidente los equipos informáticos y la información contenida en los mismos.

10. COMUNICACIÓN DE INCIDENCIAS DE SEGURIDAD

Una incidencia de seguridad se define como cualquier acción o evento, intencionado o no, que comprometa la seguridad de la información de NH, y que precise un tratamiento inmediato.

Comunica todas las incidencias de Seguridad que detectes

- Incidencias de seguridad son la detección de virus, la suplantación de tu usuario, la divulgación no autorizada de información Confidencial, el robo de equipos informáticos o soportes que te pertenezcan y que incluyan Información sensible, así como la parada de procesos críticos de negocio o soporte.
- No divulgues internamente las incidencias que detectes, ya que pueden ser Confidenciales.
- Si tienes dudas sobre si algo que has detectado es o no una incidencia, comunícala de todos modos.
- El método para gestionar las incidencias es a través del software corporativo Landesk (<https://landesksd.nh-hoteles.com/>) , en caso de no ser posible, se podrá enviar un correo a infosec@nh-hoteles.com

11. TRATAMIENTO DE DATOS DE SENSIBLES

El uso de datos sensibles, como por ejemplo los datos personales de nuestros clientes, datos de tarjeta de crédito, datos personales de los empleados, son necesarios para la correcta operativa pero requiere una serie de responsabilidades que garanticen la seguridad de estos datos.

Existen varias normativas que establecen requerimientos legales que estamos obligados a cumplir, por ejemplo la LOPD en España, estos requerimientos pasan por establecer medidas técnicas y organizativas necesarias para garantizar la seguridad que deben reunir los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal. Así como asegurar que los procesos de negocio se adaptan a los requerimientos, como garantizar que se cumplen requerimientos procedimentales con la autoridades, como por ejemplo, la inscripción de los ficheros declarando los datos que se van a procesar y con qué finalidad.

Protege la información de carácter sensible que utilices en tu trabajo en NH

- No accedas ni almacenes datos de carácter sensible si no los necesitas para desarrollar tu trabajo.
- Si creas ficheros temporales que incluyan datos sensibles, elimínalos cuando dejes de utilizarlos.
- No divulgues información de carácter sensible salvo que tengas autorización. Si detectas una divulgación no autorizada de datos sensibles, comunícalo al área de Seguridad.
- Cumple con tus responsabilidades de protección de la Seguridad de la Información cuando manejes datos de carácter sensible.

12. REVISION

Este manual deberá ser revisado de forma periódica, entre los supuestos que podrán originar su revisión se encuentran:

- Propuestas de mejora formuladas por las auditorias efectuadas.
- Cambio en la legislación vigente referente a lo que este Manual expresa.
- Cambios tecnológicos significativos.

El encargado de dicha revisión será el Responsable de Seguridad de la información.

13. Y RECUERDA QUE...

La Seguridad de la Información de NH es responsabilidad de todos. Tu compromiso y profesionalidad son la mejor protección.