DOCUMENTO DE SEGURIDAD

Anexo V – CONTROL DE ACCESO

Nivel de seguridad de la información:

Uso Interno

Localización: Departamento de Sistemas

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

Índice

1. Introducción

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 información de carácter personal, 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.

Las altas, bajas, o modificaciones de los diferentes perfiles asignados a los usuarios, se realizarán a través de los responsables adecuados, los cuales tramitarán las solicitudes siguiendo el circuito establecido.

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.

Las contraseñas de acceso a los ficheros se cambiarán con la periodicidad que se determine en el documento **A05.1 - Características técnicas y de seguridad de las aplicaciones informáticas (catálogo)**.

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

Los usuarios están obligados a poner en conocimiento del Responsable de Seguridad cualquier incidencia que afecte a la confidencialidad e integridad de los datos de un fichero.

2. Medidas generales

- El acceso a los sistemas de información es controlado mediante mecanismos que garantizan que los usuarios no accedan a los datos y recursos con privilegios distintos de los autorizados.
- El control de acceso a los datos y recursos se realizará y definirá en función de perfiles o grupos de usuarios.
- Siempre que sea posible se establecerán perfiles de usuarios que atiendan a la siguiente segregación de tareas:
  - ✓ Tareas de negocio
  - ✓ Administración del sistema
  - ✓ Operación del sistema
  - ✓ Desarrollo y mantenimiento del sistema (o aplicaciones)
  - ✓ Gestión de cambios del sistema
  - ✓ Administración de seguridad
  - ✓ Auditoria de seguridad
- Los privilegios de acceso a los datos y recursos de los sistemas de información se concederán a grupos o perfiles de usuarios y se tratará de evitar la asignación a usuarios individuales.
- Los usuarios tendrán asignados perfiles, de manera que sólo tengan los mínimos privilegios de acceso a los datos y recursos necesarios para realizar sus funciones.
- Los usuarios se crearán:
  - ✓ Usando la normativa de identificación y autenticación como se describe en el **Anexo IV.- Identificación y Autenticación**.
  - ✓ Realizando una asignación y control de privilegios de acceso.
- Existirán mecanismos para obtener la relación actualizada de los perfiles existentes, de los privilegios concedidos a cada perfil y de los usuarios pertenecientes a cada perfil.
- Los Administradores de Seguridad serán los responsables de conceder, alterar o anular el acceso autorizado o los privilegios de los usuarios, conforme a los criterios de los Responsables de Tratamiento del Fichero y del Responsable de Seguridad.
- Existirá obligatoriedad de bloqueo del puesto de trabajo, por parte del usuario, una vez finalizada la actividad del día o en ausencias prolongadas.

3. Administración de usuarios

El personal autorizado por el Responsable del Fichero: técnicos del departamento de sistemas, será el que podrá conceder, alterar o anular el acceso sobre datos y recursos, siempre bajo supervisión del Responsable de Seguridad.

Altas, bajas y modificaciones de usuarios

Se establecen las siguientes categorías de empleados:

- Interno
- Becario
- Hotel

A parte de estos tres puede existir una tipología extra de usuarios de los recursos tecnológicos que se trataran de manera diferente que son los correspondientes a:

- Personal externo

Para las tres primeras categorías se establece el siguiente procedimiento:

Hay una fase previa por parte de RRHH donde se lleva a cabo el proceso de selección para cubrir una necesidad que surja en algún departamento concreto.

Una vez concluida con éxito y con los datos del futuro empleado, éstos son introducidos por parte del departamento de RRHH en la BBDD de empleados, esta acción disparará varios procesos de provisión para ese usuario en los diferentes aplicativos necesarios según su cargo.

Esta acción automática se ve completada con acciones manuales solicitadas por el responsable a través de ServiceDesk para cubrir el resto de necesidades de permisos o aplicaciones que requieran aprobación.

En el caso de personal externo, no es el departamento de RRHH sino el departamento encargado del servicio externo el responsable de solicitar el usuario y los permisos a través de Service Desk.

Respecto las modificaciones, alguna de ellas se producirán de manera automática, a raíz de un cambio de los datos del empleado por parte del departamento de RRHH, por ejemplo, cargo, centro de trabajo, etc, otro tipo de modificaciones deberá ser solicitadas por el responsable del empleado a través de ServiceDesk para ser tramitadas una vez aprobadas.

Respecto las bajas, éstas se producirán a raíz de la eliminación del empleado de la BBDD por parte del departamento RRHH, en algunos casos, será necesario además solicitar la baja mediante ServiceDesk.

4. Revisiones Periódicas

El área de la Seguridad de la Información será el área encargada de validar, periódicamente, la necesidad de los accesos a los sistemas así como las autorizaciones que se han ido concediendo/revocando. De este modo se pretende conseguir dos objetivos principales:

- Evitar la presencia de las denominadas cuentas fantasma (ghost accounts) en los sistemas. Este tipo de cuentas son identificadores que han quedado activos –de forma intencionada o no– después del cese del propietario del mismo y cuya baja no ha sido tramitada por el responsable del departamento o por Recursos Humanos.
- Evitar el exceso de autorizaciones, siguiendo el principio del need-to-know. La rotación entre departamentos puede provocar que las autorizaciones asignadas a un identificador sobrepasen sus necesidades reales pudiendo así comprometer la seguridad de la información. El principio del need-to-know (necesidad de conocer) defiende que se concederá las autorizaciones estrictamente necesarias para el correcto desempeño de las funciones asignadas a esa cuenta.

Para ello, el Área de Seguridad de la Información procederá de la forma siguiente:

- Comprobará las cuentas activas mediante el cruce de informes de personal (trabajadores en activo) con las cuentas activas en ese momento.
- Seleccionará cuentas de acceso aleatorias y validará que las autorizaciones de las que disfruta coincide con sus necesidades, siguiendo el principio del need-to-know.
- Obtendrá una relación de usuarios que han causado baja en la compañía y comprobará que se han desactivado/cancelado todos sus identificadores.

La periodicidad establecida para llevar a cabo las revisiones dependerá de la tipología de la Información accedida, estableciéndose las siguientes directrices:

- Se procederá a la revisión formal de los derechos de acceso de los usuarios (cuentas y permisos) a Activos de Información clasificados como de Uso Interno, con una periodicidad que no superará los 6 meses.
- En el caso de Información Confidencial, se revisarán los derechos de acceso a la misma con una periodicidad mensual.

De forma adicional a lo anterior, se llevará a cabo una revisión de los perfiles de acceso definidos en los diferentes sistemas, con objeto de comprobar su adecuación a lo dispuesto por el propietario del activo. Esta revisión se realizará con una periodicidad semestral.

5. Registro de accesos

Según el artículo 24 de la LOPD, para todos los sistemas y aplicaciones que traten datos de **nivel alto** deberá implantarse un mecanismo de Registro de Accesos que recoja: ID de usuario, fecha y hora de acceso, fichero accedido, tipo de acceso y si ha sido autorizado o rechazado. Ver **A05.4 - Informe de registro de accesos a ficheros de nivel alto (registro)**.

En el caso de accesos autorizados habrá que guardar la información que permite identificar el registro accedido. El período mínimo de conservación de los datos registrados será de dos años.

Es necesario realizar una revisión periódica sobre la información registrada, así como elaborar un Informe Mensual con dichas revisiones y con los problemas detectados.

5.1 Aplicaciones afectadas

El listado de aplicaciones afectadas por este apartado del reglamento son las categorizadas como de nivel alto, en el documento **A05.3 Ficheros lógicos (catálogo)**.

5.2 Elaboración del Informe

De cada intento de acceso a las aplicaciones se recoge y conserva la siguiente información:

- Identificación del usuario
- Fecha y hora
- Fichero accedido
- Tipo de acceso
- Si el acceso ha sido autorizado o denegado
- En caso de haber sido autorizado, la información que permita identificar el registro accedido.

Este documento deberá ser revisado por el Responsable de Seguridad con carácter anual.

Los resultados del proceso de revisión deberán documentarse mediante registros e informes, con objeto de aumentar la madurez del proceso. La información a documentar será, al menos, la siguiente:

- Registro con los incumplimientos de las responsabilidades en materia de Seguridad de la Información por parte de los usuarios internos, externos y en prácticas, incluyendo toda la información asociada.

- Registro con los incumplimientos contractuales o de indicadores de Nivel de Servicio en materia de Seguridad de la Información, para cada uno de los proveedores.

- Tiempos de indisponibilidad de los sistemas de criticidad Media y Alta.

- Intentos de intrusión desde el exterior, en base a la información proporcionada por el firewall, incluyendo toda la información relativa al origen del ataque y a los destinos potenciales.

- Software malicioso detectado en la plataforma, documentando la fuente y el alcance de infección.

- 10 incidencias más críticas relativas a la Seguridad de la Información.

- Cambios relevantes en la configuración de seguridad de los diferentes equipos, especialmente en lo relativo a las reglas de filtrado del firewall y a la configuración del acceso remoto por VPN.

- Número de cuentas "fantasma" detectadas, que permitirían el acceso a Información Confidencial o de Difusión Limitada. Ver **A05.2 - Usuarios genéricos controlados (registro)**.

- Número de usuarios bloqueados en el periodo analizado, provocados por intentos incorrectos de acceso al sistema.

Con la información anterior más relevante, así como con cualquier otra que el Responsable de Seguridad de la Información pueda considerar relevante, se creará un informe detallado para cada periodo de Revisión, en el que se describirán cada uno de los puntos indicados anteriormente (ver **A05.4 - Informe de registro de accesos a ficheros de nivel alto (registro)**, para consultar la plantilla de registro, y **A03.1 Actividades de control periódicas (catálogo)**, para consultar la tarea periódica definida).