MARCO NORMATIVO DE SEGURIDAD DE LA INFORMACIÓN

Detalles de documento

Nombre del documento

Marco Normativo de Seguridad de la Información

Identificador del documento

ALLNH-NOR202-ES

Versión	Fecha	Estado
1.0	Noviembre 2018	Aprobada

Autor	Revisado por	Aprobado por
Information Security	Responsable de Information Security	Information Security

Propietario	Nivel de confidencialidad
Information Security	Uso interno

Control de versiones

Versión	Fecha	Autor	Modificaciones
1.0	Noviembre 2018	Information Security	Versión inicial

Contenido:

1. INTRODUCCIÓN

La evolución de las Tecnologías de la Información y su extensa implantación han hecho crecer de manera exponencial el riesgo que suponen las principales amenazas de estas tecnologías para las organizaciones. Este aumento del riesgo provoca la necesidad de implantar medidas de seguridad adecuadas y proporcionales que garanticen una protección integral efectiva de la información y las comunicaciones, teniendo en cuenta el dinamismo operativo y la organización de NH Hotel Group (en adelante el "Grupo NH" o "NH").

NH tiene la obligación de garantizar el cumplimiento de la legislación vigente, así como de preservar la confidencialidad, integridad y disponibilidad de la información, así como de los sistemas de información y comunicaciones que soporten o transmitan información de su titularidad o bajo su responsabilidad.

2. OBJETIVO

El objetivo del presente documento es definir los objetivos de control desarrollando cada uno de los principios de seguridad de la información detallados en la Política de Seguridad de NH.

3. ALCANCE

Las presentes normativas son de aplicación al personal del Grupo NH, de sus sociedades y de terceras entidades que en el ámbito de una relación laboral o comercial traten información titularidad o bajo la responsabilidad de NH.

En el ámbito de las normativas se incluyen los sistemas de información y comunicaciones, servicios de TI y tecnologías que soportan los procesos de negocio, servicios y funciones de NH, con independencia de la ubicación del tratamiento o del soporte o medios que contengan la información.

4. DEFINICIONES

Las definiciones y términos utilizados en las presentes normativas han sido detallados en el Glosario de términos y definiciones.

5. DETALLE

A continuación, se detallan los objetivos de control organizados por dominios de seguridad de la información:

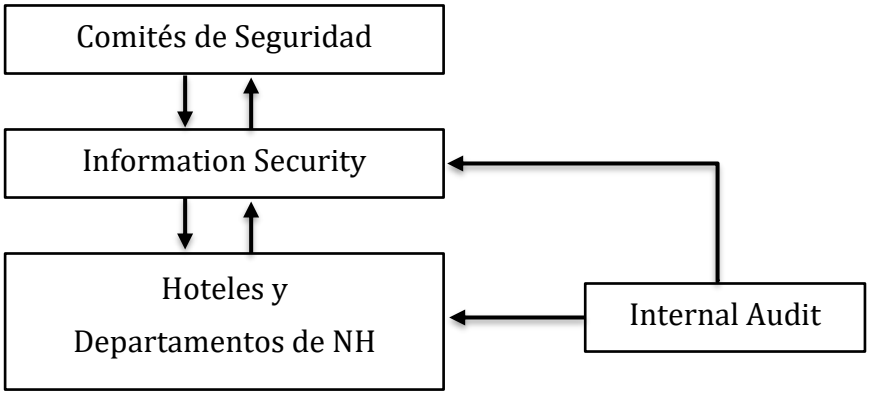
5.1. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

5.1.1. Organización interna

La protección de la información titularidad o bajo la responsabilidad de NH es una responsabilidad compartida por todos los empleados y colaboradores internos y externos.

La responsabilidad de aplicar las directrices marcadas en la Política de Seguridad de NH recae en los Directores de Hotel, en los responsables de cada departamento de NH y en los miembros de los órganos de administración de las sociedades y demás entidades que conforman el Grupo NH.

Para gobernar la seguridad de la información en el Grupo NH, la Dirección de NH ha definido y establecido la siguiente estructura organizativa sólida y compacta:



La estructura organizativa de seguridad de la información de NH cumple los siguientes principios:

- Seguridad como un proceso integral: la seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con la seguridad de la información.
- Coordinación de la gestión de la seguridad: mediante la coordinación de Information Security con las diferentes Divisiones, Departamentos, Áreas y Unidades de Negocio del Grupo NH, así como la colaboración de diferentes funciones en un proyecto común.
- Autoridad suficiente y recursos adecuados: Los Comités de Seguridad e Information Security tienen la autoridad necesaria en la organización para realizar las funciones y responsabilidades que se les han asignado, así como los recursos adecuados para llevarlas a cabo.

- Sistema efectivo de gobierno interno: las responsabilidades en materia de seguridad estarán diferenciadas y distribuidas en tres niveles diferentes denominados líneas de defensa. La primera línea de defensa consiste en los hoteles y departamentos que toman y asumen riesgos, así como limitar y llevar a cabo verificaciones operacionales y administrativas. La segunda línea de defensa contribuye al control independiente del riesgo, en la cual se encuentra Information Security. Finalmente, la tercera línea de defensa proporciona una revisión independiente, objetiva y crítica de las dos primeras líneas, y en ella se encuentra Internal Audit.

Comités de Seguridad

La organización de la seguridad de la información del Grupo NH se coordina mediante los siguientes órganos de gestión: el Comité de Seguridad y el Comité de Seguimiento de Seguridad.

Comité de Seguridad

El Comité de Seguridad, por su composición, es el órgano de decisión y gestión de mayor nivel en el Grupo NH en los asuntos relacionados con la seguridad de la información.

La misión del Comité es la mejora continua de la seguridad, garantizando un nivel mínimo homogéneo y acorde con las necesidades de cada negocio.

El funcionamiento del citado Comité se basa en los siguientes aspectos:

- El Coordinador del Comité es el Responsable de Information Security.
- El Secretario del Comité es un miembro de Information Security, el cual debe levantar actas del desarrollo de las sesiones.
- Su composición es decisión del propio Comité, atendiendo a criterios operacionales y de negocio, factores geográficos y representación suficiente de las sociedades del Grupo NH. Como mínimo, en el Comité deben estar representados:
    - Responsable de IT & Systems
    - Responsable de Legal Affairs
- Los miembros del Comité, de forma excepcional, pueden delegar su asistencia en uno de sus colaboradores.
- Los miembros de Internal Audit pueden ser invitados a las reuniones del Comité, pero exclusivamente lo harán como observadores.
- El Comité se debe reunir, como mínimo, anualmente.
- La convocatoria del Comité en pleno se debe realizar por el Secretario del Comité a instancia del Coordinador del Comité, a través de medios telemáticos acompañados del orden de la reunión, así como de la documentación necesaria para el seguimiento de la misma.

Las funciones y responsabilidades del Comité son las siguientes:

- Asumir la responsabilidad de velar por el cumplimento de los principios corporativos en materia de seguridad de la información detallados en la Política de Seguridad de NH.
- Definir las iniciativas necesarias para gestionar los riesgos en materia de seguridad de la información y continuidad de negocio, velando por el alineamiento con los objetivos de negocio del Grupo NH.

- Proponer a la Dirección de NH cambios en la Política de Seguridad, así como principios de seguridad de la información, que aseguren su idoneidad y eficacia.
- Revisión periódica de la Política de Seguridad, de manera previa a que la Dirección de NH la revise y la apruebe.
- Velar e impulsar el cumplimiento de la Política de Seguridad y de los estándares normativos que se emanan de esta y que sean de obligado cumplimiento para todo el Grupo NH, así como de su desarrollo normativo.
- Aprobar y asegurar el cumplimiento de una estrategia integral de seguridad que esté vinculada de manera intrínseca con los objetivos de negocio, definiendo anualmente unos objetivos corporativos de seguridad de la información.
- Reportar periódicamente a la Dirección de NH, el estado de los objetivos corporativos en materia de seguridad de la información y los riesgos residuales.
- Asignar recursos necesarios para planificar, implantar, operar, supervisar, revisar, mantener y mejorar la gestión de la seguridad de la información.
- Aprobar la asignación inicial y revisión periódica de roles y responsabilidades en materia de seguridad de la información, así como establecer los criterios que garanticen la segregación de funciones.
- Establecer un plan de formación y capacitación en materia de seguridad de la información para todos los empleados de NH.
- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones legales, regulatorias y contractuales del Grupo NH en materia de seguridad de la información.

Comité de Seguimiento de Seguridad

El Comité de Seguimiento de Seguridad, por su composición, es el órgano encargado de realizar un seguimiento más exhaustivo de las diferentes iniciativas relacionadas con seguridad de la información en Grupo NH.

La misión del Comité de Seguimiento es la mejora continua de la seguridad, garantizando una involucración de IT & Systems, más concretamente las Áreas de Applications e Infrastrucure.

El funcionamiento del citado Comité de Seguimiento se basa en los siguientes aspectos:

- El Coordinador del Comité de Seguimiento es el Responsable de IT & Systems.
- El Secretario del Comité de Seguimiento es un miembro de Information Security, el cual debe levantar actas del desarrollo de las sesiones.
- Su composición es decisión del propio Comité de Seguimiento, atendiendo a criterios operacionales y de negocio, factores geográficos y representación suficiente de las sociedades del Grupo NH. Como mínimo, en el Comité de Seguimiento deben estar representados:
    - Responsable de IT & Systems
    - Responsable de Applications de IT & Systems
    - Responsable de Infrastructure de IT & Systems
- Los miembros del Comité de Seguimiento, de forma excepcional, pueden delegar su asistencia en uno de sus colaboradores.
- El Comité de Seguimiento se debe reunir, como mínimo, trimestralmente.

- La convocatoria del Comité de Seguimiento en pleno se debe realizar por el Secretario del Comité a instancia del Coordinador del Comité, a través de medios telemáticos acompañados del orden de la reunión, así como de la documentación necesaria para el seguimiento de la misma.

Las funciones y responsabilidades del Comité son las siguientes:

- Revisar y aprobar los estándares normativos de seguridad emanados de la Política de Seguridad que sean de obligado cumplimiento para el Grupo NH.
- Proponer al Comité de Seguridad la asignación de los recursos necesarios para planificar, implantar, operar, supervisar, revisar, mantener y mejorar la gestión de la seguridad de la información y el cumplimiento de leyes, regulaciones y obligaciones contractuales en materia de seguridad de la información.
- Aprobar la asignación inicial y revisión periódica de roles y responsabilidades, así como establecer los criterios que garanticen la segregación de tareas.
- Priorizar las actuaciones en materia de seguridad de la información cuando los recursos sean limitados.
- Revisar el desarrollo de los proyectos de gestión de riesgos aprobados.
- Informar regularmente del estado de la seguridad de la información en el Grupo NH al Comité de Seguridad.
- Promover la mejora continua en la gestión de la seguridad de la información.
- Coordinar los Planes de Continuidad de las Divisiones, Departamentos, Áreas y Unidades de Negocio del Grupo NH, para asegurar una actuación sin fisuras en el caso de que deban ser activados.
- Promover la realización de revisiones periódicas que permitan verificar el cumplimiento de las obligaciones legales, regulatorias y contractuales del Grupo NH en materia de seguridad de la información.

Information Security

Information Security es el Área del Grupo NH encargada de velar por el cumplimiento y mantenimiento de la Política de Seguridad de NH.

Las funciones y responsabilidades de Information Security son las siguientes:

- Informar del estado de la seguridad de la información en el Grupo NH al Comité de Seguridad.
- Promover y defender las directrices de seguridad de la información de NH, con el fin de que éstas estén alineadas con las necesidades de negocio del Grupo NH.
- Desarrollo de la Política de Seguridad, asegurando su implantación y alineamiento con la resta de cuerpos normativos del Grupo NH.
- Realizar análisis de riesgos, con el fin de definir las medidas de seguridad organizativas y técnicas necesarias y proporcionales que mitiguen los riesgos a los que el Grupo NH está expuesto.
- Proporcionar soporte durante la implantación de las medidas de seguridad organizativas y técnicas.
- Velar por la implantación de las medidas de seguridad organizativas y técnicas que den cumplimiento a los estándares normativos de seguridad.
- Seguimiento del cumplimiento de los controles de seguridad definidos en los estándares normativos que desarrollan la Política de Seguridad.
- Definir y gestionar las métricas y los reportes en materia de seguridad de la información.
- Definir los procedimientos necesarios para la gestión de crisis y garantizar la continuidad de negocio.

- Definir y gestionar el Plan de formación y concienciación en materia de seguridad de la información del Grupo NH.
- Definir y gestionar los planes anuales de revisiones y análisis exhaustivos de seguridad de los sistemas de información y comunicaciones y de los servicios de TI de NH.
- Definir y operar los sistemas de seguridad implantados en el Grupo NH que monitoricen y controlen el correcto funcionamiento de sistemas de información y comunicaciones de los servicios de TI de NH.
- Gestionar y dar respuesta a las incidencias de seguridad de la información. En caso de ser necesario, coordinar los análisis informáticos forenses.
- Gestionar las peticiones, problemas y cambios en materia de seguridad de la información.
- Gestionar las identidades y el control de acceso en herramientas corporativas.
- Establecer y mantener contacto con grupos de interés y foros especializados en seguridad de la información.

Asimismo, Information Security debe establecer contacto con autoridades y grupos de especial interés en materia de seguridad de la información, de manera que pueda aumentar su nivel de excelencia en la citada materia, estar al corriente de las últimas tendencias y compartir el conocimiento en foros sectoriales. Por ello, Information Security interactúa con:

- Asociaciones profesionales en materia de seguridad de la información (p.e., ISACA – Information Systems Audit and Control Association, ISMS Forum, CSA – Cloud Secure Alliance, etc.)
- Organismos públicos relacionados con la seguridad de la información (p.e., INCIBE - Instituto Nacional de Ciberseguridad, CCN-CERT – Centro Criptológico Nacional - Computer Emergency Response Team, ENISA - European Union Agency for Network and Information Security, etc.)
- Congresos relacionados con la seguridad de la información, organizados por asociaciones profesionales, empresas del sector privado, organismos públicos o asociaciones sin ánimo de lucro.
- Fuerzas y Cuerpos de Seguridad del Estado en la investigación de incidentes de seguridad de la información, incluyendo fugas de información (p.e., EC3 Europol European Cybercrime Centre, GDT - Grupo de Delitos Telemáticos de la Guardia Civil de España, etc.)

El Responsable de Information Security es el responsable de Information Security. Por ello, es el responsable de gestionar las funciones y responsabilidades de Information Security, anteriormente citadas.

Hoteles y Departamentos de NH

Personal de hoteles y miembros de Departamentos

El personal de hoteles y los miembros de los Departamentos, con independencia de que sean empleados o colaboradores internos o externos, que traten información titularidad o bajo la responsabilidad de NH, tienen las siguientes funciones y responsabilidades en materia de seguridad de la información:

- Asegurarse de leer, comprender y cumplir con la Política de Seguridad de NH, así como los estándares normativos que emanan de la misma.
- Proteger activamente los activos de información que les sean asignados.
- Garantizar la confidencialidad e integridad de la información a la que tienen acceso, conocer y aplicar los criterios de clasificación de la información y las medidas para su adecuado tratamiento.

- Garantizar la confidencialidad de las credenciales de acceso proporcionadas por NH que le fueran asignadas.
- Informar de cualquier incidente de seguridad o acontecimiento inusual que sea observado durante la operación de los sistemas de información y comunicaciones de NH, así como los servicios de TI.

Directores de Hoteles y responsables de Departamentos

Los Directores de Hoteles y los responsables de Departamentos, o las personas designadas por éste, deben asumir las siguientes funciones y responsabilidades en materia de seguridad de la información:

- Definir el uso adecuado de los activos de información bajo su responsabilidad.
- Autorizar el uso de activos de información a los empleados y colaboradores internos y externos del Grupo NH.
- Garantizar que todos los empleados y colaboradores internos y externos que organizativamente pertenecen o prestan servicios al Hotel o Departamento, conocen y aplican la Política de Seguridad de NH.
- Velar para la adecuación de los análisis de riesgos y las medidas de seguridad organizativas y técnicas sean implantados en su Hotel o Departamento, así como desarrollar los procedimientos de seguridad de la información necesarios para adecuar la Política de Seguridad de NH a su operativa diaria, notificando a Information Security cualquier situación que requiera una modificación sustancial con respecto a lo indicado en los estándares normativos de seguridad.
- Coordinar y gestionar de forma adecuada el tratamiento de la información dentro de su División, Departamento, Área o Unidad de Negocio.
- Coordinan los proyectos de seguridad asignados, total o parcialmente, a su División, Departamento, Área o Unidad de Negocio.
- Los empleados de NH que ostenten los roles de propietario de la información o responsable de proceso de negocio, de acuerdo con los estándares normativos de seguridad, son los dueños de los riesgos de la información y de los riesgos de los procesos de negocio.

IT & Systems

Las funciones y responsabilidades de IT & Systems en materia de seguridad de la información son las siguientes:

- Colaborar con el Responsable de Information Security para coordinar y controlar las medidas de seguridad organizativas y técnicas aplicables a los sistemas de información y comunicaciones, asegurando el buen funcionamiento del proceso de gestión de la seguridad.
- Asegurar el análisis, diseño, codificación, pruebas y mantenimiento de los productos de software, para satisfacer las necesidades de clientes y usuarios, garantizando el cumplimiento de los requisitos de seguridad establecidos en los estándares normativos.
- Aplicar o colaborar en la aplicación de controles y medidas de seguridad organizativas y técnicas que aseguren la confidencialidad, integridad y disponibilidad de los activos de información de NH a lo largo de su ciclo de vida.
- Soporte en la selección, implantación, configuración y operación de los mecanismos y herramientas adecuadas que permitan aplicar la Política de Seguridad.

- Definir políticas y procedimientos para asegurar el cumplimiento de las funciones y responsabilidades asignadas a IT & Systems en la Política de Seguridad de NH, así como los estándares normativos que emanen de la misma.
- Establecer Planes de continuidad, llevando a cabo pruebas periódicas para garantizar su eficacia.
- Notificar los incidentes de seguridad que afecten a sistemas de información y comunicaciones de su responsabilidad, así como colaborar en su investigación.

Legal Affairs & Compliance

Las funciones y responsabilidades de Legal Affairs & Compliance en materia de seguridad de la información son las siguientes:

- Asesorar en relación a los requerimientos legales, regulatorios y contractuales en materia de seguridad de la información a los que se encuentra sujeto el Grupo NH.
- Colaborar y dar apoyo en identificar las iniciativas que Information Security debe coordinar o estar involucrado, las cuales sirvan para supervisar el funcionamiento y el cumplimiento del modelo de prevención penal implantado en NH.

Operations

Las funciones y responsabilidades de Operations en materia de seguridad de la información son las siguientes:

- Definir e implementar las medidas de control de acceso físico a los edificios de NH.
- Establecer y mantener la relación con las Fuerzas y Cuerpos de Seguridad del Estado.

People

Las funciones y responsabilidades de People en materia de seguridad de la información son las siguientes:

- Determinar los perfiles y responsabilidades en el proceso de selección de los empleados, así como revisar y verificar los datos de los trabajadores antes de la contratación.
- Establecer los procesos disciplinarios internos.
- Determinar las responsabilidades de los empleados en el caso de extinción de la relación laboral, de acuerdo con la Política de Seguridad de NH.
- Iniciar el proceso de retirada de los derechos de acceso a la información de NH a los empleados en el caso de extinción de la relación laboral.
- Asegurar la firma de los acuerdos de confidencialidad y cláusulas contractuales en materia de seguridad de la información, así como de privacidad, entre el Grupo NH y los empleados de manera previa a su incorporación.

Internal Audit

Internal Audit es la función que garantiza la objetividad, independencia y confidencialidad de los procesos de auditoría del Grupo NH.

Las funciones y responsabilidades de Internal Audit, en relación con la seguridad de la información, son las siguientes:

- Proporciona aseguramiento en la evaluación de la eficacia de la gestión de los riesgos de seguridad y de los controles implantados en esta materia.
- Evaluar el funcionamiento de controles de seguridad implantados mediante auditorías y emitir una opinión en base a los riesgos asociados y los hallazgos detectados, estableciendo las recomendaciones oportunas.
- Promover la inclusión en el Plan de auditoría del Grupo NH, el cual es aprobado por el Comité de Auditoría y Control, las auditorías oportunas en base a los análisis de riesgos realizados por Information Security, así como por los análisis de riesgos propios.
- Colaborar con Information Security para el alineamiento con el Modelo de Aseguramiento Corporativo de NH.
- Asistir como invitado y observador a Comités de Seguridad, para identificar periódicamente actividades en el ámbito de la seguridad del Grupo NH.
- Realizar el seguimiento de las deficiencias o recomendaciones identificadas.

5.1.2. Análisis y gestión de riesgos

Information Security utiliza una metodología de análisis y gestión de riesgos de seguridad de la información que tiene en cuenta la sensibilidad y criticidad de los activos de información. A través de la citada metodología, se identifican las medidas de seguridad organizativas y técnicas necesarias para mitigar los riesgos identificados.

El alcance de dicha metodología afecta únicamente a los riesgos de seguridad de la información y no a otros tipos de riesgos que puedan afectar al Grupo NH (p.e., crédito, mercado, fraude, etc.)

En base a los objetivos de control de los dominios de seguridad de la ISO/IEC 27001, se realiza una evaluación del grado de madurez de los procesos y sistemas dentro del alcance. Se identifican las amenazas y vulnerabilidades a las que los procesos y sistemas dentro del alcance están expuestos. Se determina el umbral de riesgo admisible y se establecen planes de acción para minimizar el impacto de los riesgos a mitigar. Todos los riesgos cuyo nivel de madurez sea superior al umbral de riesgo admisible, Information Security y los Departamentos interesados (p.e., IT & Systems, Dirección de hoteles, etc.) son responsable de establecer los controles de seguridad y las acciones necesarias que permitan la mejora del nivel de madurez. Una vez diseñado un plan de acción, el Comité de Seguridad es el encargado de aprobarlo.

5.1.3. Seguridad de la información en la gestión de proyectos

Los Hoteles y Departamentos de NH son los responsables de la planificación y ejecución de sus proyectos.

Todos los proyectos o tareas que necesiten un desarrollo tecnológico, implican necesariamente la involucración de IT & Systems, en el ciclo de vida de dicho proyecto o tarea. IT & Systems debe involucrar cuando lo crean necesario a Information Security.

IT & Systems debe involucrar a Information Security cuando se cumpla uno de los siguientes criterios:

- El proyecto o tarea requiere la implantación de un nuevo sistema de información o modificaciones sobre uno existente.
- El proyecto o tarea requiere la contratación de un servicio a un proveedor externo al Grupo NH.

Por otro lado, la inclusión de Information Security puede ser también necesaria a consecuencia de cambios normativos que afecten a la seguridad de la información de NH. Cuando Legal Affairs, Compliance y/o el Delegado de Protección de Datos (DPD o DPO) del Grupo NH detecten esa casuística en algún proyecto o tarea, debe notificar a Information Security.

5.1.4. Dispositivos móviles

Dispositivos móviles corporativos

De manera previa a la entrega de un dispositivo móvil corporativo, los empleados y colaboradores internos y externos deben firmar un documento en el que acepten cláusulas legales relativas al uso aceptable de los equipos y dispositivos móviles (tales como ordenadores portátiles, teléfonos, tabletas, etc.) corporativos de NH.

Los empleados y colaboradores internos y externos deben tener en consideración los siguientes aspectos cuando utilicen un dispositivo móvil corporativo de NH:

- Nunca perder de vista el dispositivo.
- Activar, y mantener activado, el bloqueo del dispositivo cada 10 minutos de inactividad, y la solicitud de una contraseña o control biométrico para desbloquear el terminal.
- Utilizar contraseñas complejas y robustas para proteger el dispositivo.
- No liberar, ni manipular, los componentes del dispositivo.
- No abrir, ni aceptar, archivos de remitentes que no conozca.
- Instalar software autorizado previamente por NH.
- No instalar aplicaciones de procedencia desconocida o no fiable.
- No usar tarjetas de memoria externas y extraíbles.
- Activar, y mantener activado, el sistema de borrado remoto, siempre que sea posible.
- No dejar activados protocolos de comunicación en caso de no estar usándolos. En especial, desactivar el Bluetooth y el WiFi si no se utilizan.
- No conectarse a puntos de acceso inalámbricos (redes WiFi) no conocidos.

Un agente de una solución de gestión de dispositivos móviles (MDM) podrá ser instalado para asegurar, monitorizar y administrar los dispositivos móviles corporativos de manera remota. Dicho agente será instalado bajo petición de Information Security. El agente proporcionará las siguientes funcionalidades:

- Instalación y ejecución de aplicaciones de manera remota.
- Aplicación de políticas de control sobre el dispositivo y aplicaciones.
- Localización remota del dispositivo.
- Bloqueo remoto del dispositivo o de funciones.
- Borrado remoto de información.

- Escaneo automático de virus o programas maliciosos.

Dispositivos móviles no corporativos

Salvo autorización expresa, no se deben utilizar dispositivos no corporativos (es decir, dispositivos personales, de terceros o que no sean propiedad del Grupo NH) para el tratamiento o almacenamiento de información titularidad o bajo la responsabilidad de NH.

En caso de que se haya autorizado, Information Security deben aprobar los dispositivos no corporativos de manera previa al inicio del tratamiento o almacenamiento de información de NH.

Los empleados y colaboradores internos y externos deben garantizar los siguientes aspectos en los dispositivos no corporativos:

- El uso de los dispositivos debe adherirse a las políticas internas de NH (especialmente, a las políticas de Recursos Humanos o People) y a los requerimientos legales y reglamentarios vigentes y aplicables.
- El dispositivo no se debe compartir con otra persona (especialmente con familiares, amigos, etc.)
- Los dispositivos se deben custodiar y proteger fuera de las instalaciones de NH.
- En caso de pérdida o robo del dispositivo, se debe notificar inmediatamente a Information Security a través del correo electrónico infosec@nh-hotels.com.

También, los empleados y colaboradores internos y externos deben asegurarse que los dispositivos están configurados para cumplir con los siguientes aspectos:

- Los dispositivos deben tener instalado en todo momento un sistema operativo original proporcionado por el fabricante o desarrollador (es decir, que no sea hayan modificado los sistemas operativos, sean dispositivos rooted o jailbroken, etc.)
- El sistema operativo de los dispositivos debe mantenerse actualizado de acuerdo con las especificaciones del fabricante o desarrollador.
- Las contraseñas de los dispositivos deben configurarse de acuerdo con los requisitos definidos en la presente Política de Seguridad de NH. Especialmente, en lo relativo a longitud mínima, complejidad, etc.
- Los dispositivos deben configurarse para forzar sistemáticamente el bloqueo de la pantalla después de diez (10) minutos de inactividad.
- Los dispositivos móviles deben configurarse para aplicar automáticamente el borrado de toda la información almacenada después de diez (10) intentos fallidos de inicio de sesión. Este borrado debe devolver el dispositivo a su configuración original de fábrica.
- Los dispositivos deben tener instalada y en uso en todo momento, una solución de cifrado de disco completo aprobada.
- Los dispositivos deben tener una solución anti-malware / antivirus instalada y actualizada.

Adicionalmente, Information Security puede requerir que la instalación de un agente de una solución de gestión de datos móviles (MDM) en el dispositivo móvil.

NH debe solicitar el acceso a los dispositivos no corporativos y debe proteger en todo momento la privacidad de dichos dispositivos.

5.1.5. Teletrabajo

Exclusivamente los empleados y colaboradores internos y externos previamente autorizados pueden realizar teletrabajo, es decir, conectarse a los sistemas de información y comunicaciones de NH desde un lugar situado fuera de las instalaciones del Grupo NH permitiendo trabajar con las mismas condiciones como si se encontrara físicamente en las propias instalaciones de NH.

Los empleados y colaboradores internos y externos deben garantizar los siguientes aspectos en relación con el teletrabajo:

- La conexión a los sistemas de información y comunicaciones de NH debe realizarse mediante una VPN autorizada por NH. En ningún caso, se podrá establecer conexiones con sistemas de NH desde una red pública (como Internet) sin haber sido autenticado en un servicio de VPN autorizado por NH.
- Nunca perder de vista el dispositivo cuando el dispositivo esté conectado a sistemas de información y comunicaciones de NH.
- En lugares públicos o con personas ajenas a NH, utilizar filtros de privacidad en las pantallas de los dispositivos.
- Impedir a personas no autorizadas por NH que manipulen el dispositivo.
- De manera previa a la conexión a los sistemas de información y comunicaciones de NH, se debe asegurar de que el antivirus esté activo y actualizado.
- No conectarse a puntos de acceso inalámbricos (redes WiFi) no conocidos.
- No se debe copiar, mover y almacenar información clasificada como Restringida o Confidencial en las unidades de disco locales y en dispositivos electrónicos extraíbles, a menos que sea autorizado explícitamente. Está expresamente prohibido copiar, mover y almacenar datos de pago (p.e., números de cuenta, números de tarjetas bancarias, nombres de titulares, códigos de servicio, fechas de vencimientos, etc.)

5.2. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS

5.2.1. Antes del empleo

NH, para el correcto desempeño de sus funciones de negocio, precisar de la contratación de empleados y colaboradores internos y externos, entre los que se incluyen las siguientes personas físicas o jurídicas:

- Empleados del Grupo NH, con independencia de la modalidad contractual que determine su relación laboral, posición que ocupen o ámbito geográfico en el que desempeñen su trabajo.
- Estudiantes en prácticas.
- Directivos del Grupo NH, con independencia de la modalidad contractual que determine su relación laboral o mercantil, posición que ocupen o ámbito geográfico en el que desempeñen su trabajo. Serán

considerados directivos en todo caso, los miembros de la Alta Dirección (definidos como aquéllos que tengan dependencia directa del Consejo de Administración o del primer ejecutivo de la Compañía y, en todo caso, el auditor interno), todos los directores y responsables de departamento y los directores de hotel.

- Miembros de los órganos de administración de las sociedades y demás entidades que conforman el Grupo NH, sea cual sea la composición, forma y régimen de funcionamiento del órgano en cuestión de que se trate.
- Proveedores, colaboradores y cualquier otro grupo de interés que, aunque no se mencionen de forma específica, tuviera vinculación directa con las operaciones del Grupo NH.

Investigación de antecedentes

En la convocatoria de un puesto a cubrir deben constar los requisitos de seguridad considerados relevantes.

En el momento en el que se obtenga un currículum vitae con datos identificativos de un candidato, Recursos Humanos (o People) del Grupo NH debe facilitar al interesado la información indicada a continuación:

- Identidad del responsable del tratamiento de datos personales (en la mayoría de los casos, la razón social del Grupo NH).
- Descripción sencilla de los fines del tratamiento de los datos personales.
- Base jurídica del tratamiento de los datos personales.
- Previsión, o no, de cesiones o transferencias a terceros países.
- Referencia al ejercicio del derecho a solicitar al responsable del tratamiento el acceso a los datos personales, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos; así como el derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada; o el derecho a presentar una reclamación ante una autoridad de control.
- En caso de que la información no proceda del interesado, la fuente de los datos.
- Asimismo, se debe hacer referencia a dónde el interesado puede encontrar la siguiente información adicional:
    - Datos de contacto del responsable del tratamiento de datos personales (en la mayoría de los casos, la dirección postal corporativa del Grupo NH).
    - Los datos de contacto del delegado de protección de datos, en caso de que NH lo haya designado.
    - Descripción ampliada de los fines del tratamiento.
    - Plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.
    - Si se van a realizar decisiones automatizadas, los perfiles y la lógica aplicada.
    - Informar de las posibles consecuencias de no facilitar los datos personales solicitados por NH, ya que la comunicación de dichos datos es un requisito necesario para poder suscribir un contrato.
    - Destinatarios o categorías de destinatarios de las cesiones de datos personales.
    - Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables en las transferencias a terceros países.
    - Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de los datos personales, y la limitación u oposición al tratamiento.

- Cómo ejercer el derecho a retirar el consentimiento prestado.
- Cómo ejercer el derecho a reclamar ante una Autoridad de Control de un Estado Miembro de la Unión Europea.
- En caso de que la información no proceda del interesado, información detallada del origen de los datos, incluso si proceden de fuentes de acceso público.
- En caso de que la información no proceda del interesado, categorías de datos que se tratan.

Durante el proceso de selección de candidatos, Recursos Humanos de NH debe realizar, si aplica, la comprobación de las referencias, especialmente las experiencias laborales y formaciones. Las citadas comprobaciones se deben realizar de acuerdo con la legislación vigente y aplicable, así como los códigos éticos internos de NH, de una manera proporcional a la clasificación de la información a la que se requiere acceder.

Términos y condiciones del empleo

Como parte de sus obligaciones contractuales, los empleados deben aceptar y firmar los términos y condiciones del contrato de trabajo, el cual debe establecer sus responsabilidades en el cumplimiento del Código de Conducta y de los procedimientos internos en materia de seguridad de la información, e incluir cláusulas contractuales sobre confidencialidad y deber de secreto. Cabe destacar que el Código de Conducta del Grupo NH establece, entre otros, la responsabilidad del empleado en relación a la confidencialidad de la información de NH.

Concretamente, el clausulado contractual debe desarrollar los siguientes aspectos:

- Información sobre los tratamientos de datos personales.
  - En particular, el empleado debe autorizar al Grupo NH a tratar sus datos personales con las siguientes finalidades: confeccionar nóminas y gestión de pago de las mismas, y realizar aquellas actividades que resulten necesarias de acuerdo con lo previsto en las leyes y regulaciones aplicables en materia de prevención de riesgos y vigilancia de la salud.
  - En el supuesto de que fuere necesario solicitar acreditaciones para eventos o ante entidades privadas o Administraciones Públicas, el trabajador debe autorizar al Grupo NH a comunicar sus los datos requeridos por terceros exclusivamente para la finalidad indicada.
- Funciones y obligaciones en relación con tratamientos de datos personales.
- Deber de secreto profesional y deber legal de guardar absoluta reserva respecto a los datos a los que el empleado tuviera acceso o conocimiento de los mismos.
  - Asimismo, los empleados deben ser informados que se encuentran sujetos al deber de confidencialidad incluso tras la finalización de su relación laboral con el Grupo NH, según lo establecido en el derecho genérico de "buena fe contractual" incluido tanto en el Estatuto de los Trabajadores (Art. 5.a) como en el Código Civil (Arts. 1258 y 7.1).
- Funciones y obligaciones emanadas de la Política de Seguridad de NH, especialmente aspectos relativos a:
  - Gestión de credenciales
  - Confidencialidad de la información
  - Gestión de incidencias de seguridad
  - Propiedad intelectual e industrial
  - Uso y retirada de equipos y dispositivos
  - Copias de respaldo
  - Uso del acceso a Internet, correo electrónico y herramientas colaborativas

- Proceso disciplinario o sancionador ante incumplimientos de leyes y reglamentes vigentes y aplicables, así como códigos y normas internas del Grupo NH, en materia de seguridad de la información.

5.2.2. Durante el empleo

Responsabilidades y obligaciones durante el empleo

Los empleados y colaboradores internos y externos deben ser respetuosos y éticos en todas las comunicaciones que realicen, teniendo siempre presente que están representando a NH. Asimismo, se debe declinar realizar cualquier declaración a un medio de comunicación, remitiendo la consulta al Departamento de Comunicación del Grupo NH.

Los empleados y colaboradores internos y externos deben abstenerse de tratar información de NH en lugares públicos o privados en los que puedan ser escuchados por terceras personas que no tienen acceso a dicha información.

Los empleados y colaboradores internos y externos tienen prohibido comunicar a un tercero ajeno a NH información sobre los clientes o empleados del Grupo NH. Está especialmente prohibido comunicar estancias en instalaciones del Grupo NH, horarios o facilitar información de contacto a terceros que se identifican como familiares o amistades de clientes o empleados de NH.

Se prohíbe explícitamente el envío o reenvío de información discriminatoria, cartas en cadena y material obsceno o de mal gusto.

Information Security debe evaluar de forma periódica el cumplimiento de las responsabilidades en materia de seguridad de la información de los empleados y colaboradores internos y externos.

Proceso disciplinario

Los empleados y colaboradores internos y externos pueden ser sancionados en virtud de incumplimientos laborales, de acuerdo con la graduación de faltas y sanciones que se establecen en las disposiciones legales o en el convenio colectivo que sea aplicable.

La valoración de las faltas y las correspondientes sanciones es responsabilidad de People (Recursos Humanos). El citado Departamento, como máximo órgano responsable, debe acordar la medida disciplinaria correspondiente en caso de que una investigación sobre los hechos denunciados se pueda concluir como un incumplimiento de la normativa interna o externa.

Formación y concienciación

Talent, Learning & Development e Information Security deben proporcionar a los empleados la formación y herramientas que sean necesarias para garantizar, en función de su actividad laboral, el correcto cumplimiento de las responsabilidades que les han sido asignadas en materia de seguridad de la información.

De manera general, se contemplarán los siguientes tipos de actividades formativas:

- De concienciación, respecto a los riesgos a los que se encuentra sometida la información de NH y las buenas prácticas y normas a considerar en el manejo de la información (p.e., alertas y píldoras de seguridad, boletines, noticias, etc.)
- De formación general, respecto a los procedimientos operativos de seguridad a considerar en el manejo de la información (p.e., manejo de las herramientas de intercambio seguro de la información, cómo reportar incidencias de seguridad, cómo cifrar o firmar correos electrónicos, etc.)
- De formación técnica, para el personal de IT & Systems, relacionado con aspectos directamente relacionados con la operación y mantenimiento seguro de los sistemas y aplicaciones. Asimismo, también se debe considerar implantar formación técnica a los miembros de Information Security, tal como asistir periódicamente a cursos o charlas en materia de seguridad de la información que se imparten en foros especializados.

El Comité de Seguridad, a propuesta del Comité de Seguimiento de Seguridad, debe aprobar un Plan de formación y capacitación en materia de seguridad que incluya sesiones de formación en seguridad de los sistemas de información para los empleados, píldoras formativas y campañas de concienciación. El citado Plan debe tener una proyección anual y podrá ser revisado con posterioridad si se considerara necesario, a fin de incorporar o sustituir iniciativas formativas. Asimismo, el Comité de Seguimiento de Seguridad debe evaluar los resultados obtenidos, de forma que se pueda medir de manera objetiva la efectividad de las acciones formativas realizadas y contribuir al proceso de mejora continua de la seguridad del Grupo NH.

5.2.3. Finalización del empleo o cambio en el puesto de trabajo

Devolución o baja de activos de información

Ya sea por decisión de NH, del empleado o colaborador, o de ambas partes, la finalización de la relación laboral se debe realizar conforme a lo expuesto el convenio colectivo que sea aplicable o, en su defecto, en el Estatuto de los Trabajadores.

El responsable directo del empleado o colaborador afectado debe notificar la decisión a Recursos Humanos del Grupo NH.

Los empleados y colaboradores internos y externos deben devolver todos los activos de NH, especialmente las credenciales de usuario, que estén en su poder al finalizar su empleo o cambio en el puesto de trabajo. Recursos Humanos debe coordinar la devolución de activos de información físicos.

Asimismo, Recursos Humanos debe notificar con la mayor antelación posible a IT & Systems y a Information Security la necesidad de tramitar la supresión de permisos de acceso a los sistemas de información y comunicaciones del Grupo NH. IT & Systems y Information Security deben comunicar a Recursos Humanos cuando los permisos de acceso hayan sido retirados.

Cambio en el puesto de trabajo

Los cambios en el puesto de trabajo dentro del Grupo NH, tales como promociones o reubicaciones, no se consideran casos de finalización del empleado. Si bien, Recursos Humanos debe notificar a IT & Systems y a

Information Security para garantizar la tramitación de la supresión de permisos de acceso a los sistemas de información y comunicaciones del Grupo NH.

Acuerdos de confidencialidad tras la finalización del empleo

Según lo establecido en el convenio colectivo que sea aplicable, ante una falta grave o violación de las leyes o regulaciones aplicables, así como de las normas internas del Grupo NH, puede ser aplicado un proceso disciplinario que podría derivar en despido. La necesidad de iniciar acciones legales debe ser valorada por la Dirección de NH, Legal Affairs y Recursos Humanos del Grupo NH, tomándose las medidas oportunas en base a las leyes y regulaciones vigentes y aplicables.

En caso de detectarse incumplimientos de los acuerdos de confidencialidad que pudieran comprometer la seguridad de la información del Grupo NH, Legal Affairs y Recursos Humanos deben poner en conocimiento al Comité de Seguridad.

5.3. GESTIÓN DE ACTIVOS

5.3.1. Responsabilidad sobre los activos

Inventario de activos de información

Los activos de información de NH deben estar identificados e inventariados.

El inventario de activos de información del Grupo NH debe ser mantenido por IT & Systems. Este inventario debe mantener toda la información relevante mínima para poder realizar una adecuada gestión de la seguridad de la información. Entre otros, esta base de datos contendrá información sobre la dirección IP y/o la URL del activo de información, el sistema operativo, la versión del mismo, e interdependencias con otros activos. Asimismo, debe indicarse la información de contacto del propietario del activo de información.

Propiedad de los activos

NH es propietario de todos los activos de información puestos a disposición de sus empleados para el ejercicio de sus funciones.

La información de NH debe tener asignada un propietario de la información. Éste debe ser empleado interno del Grupo NH.

El propietario de la información es el responsable de definir para que usos y finalidades se puede tratar la información de la cual son responsables.

El propietario de la información es responsable de su clasificación y protección de acuerdo con la Política de Seguridad de NH.

Uso aceptable de los activos de información

Los usuarios de los activos de información de NH son responsables de asegurar que se hace un uso de dichos activos conforme a la Política de Seguridad de NH y a la legislación vigente y aplicable. De manera general, el uso de los activos de información de NH para propósitos que no estén aprobados o autorizados como operaciones o actividades del Grupo NH, constituye un mal uso de los mismos.

Está expresamente prohibido el uso de la información y los activos de información de NH para finalidades distintas a las estrictamente relacionadas con el desempeño habitual de las funciones y responsabilidades laborales en NH. Asimismo, su uso es susceptible de ser monitorizado y auditado por parte de NH, dentro de los límites marcados por la legislación vigente.

El uso de los servicios de TI corporativos, como la navegación por Internet o el servicio de correo electrónico, debe estar restringido al personal que estrictamente lo necesite para llevar a cabo su actividad laboral.

La instalación de software en equipos o dispositivos de NH que no se encuentren debidamente autorizadas por NH, así como la modificación de configuraciones y la instalación y ejecución de programas maliciosos, queda prohibida.

Salvo autorización expresa, los equipos o dispositivos de colaboradores externos no se deben conectar a las redes corporativas de NH personales o de terceros. Especialmente, se prohíbe expresamente la conexión de equipos o dispositivos de los colaboradores externos a los equipos de comunicación de NH en los hoteles sin la autorización previa.

5.3.2. Clasificación de la información

Tipos de activos de información

Se entiende por activos de información primarios:

- Información generada por medios propios o por terceros que dan soporte a las funciones y servicios del Grupo NH, con independencia del soporte o los medios que la contengan.
- Sistemas de información y servicios de TI que dan soporte a la gestión de la actividad y/o la prestación de servicios del Grupo NH y que la información que tratan no se puede clasificar como activo de información primario.

Se entiende por activo de información de soporte:

- Estructuras de datos en las que se mantiene información, tales como bases de datos, ficheros, gestores documentales.
- Servidores y sistemas en los que se almacena información.
- Sistemas de información y servicios de TI utilizados para el tratamiento de información.
- Equipos y sistemas de comunicaciones entre los sistemas de información, servicios de TI o sistemas de terceros.
- Hardware o soportes que permite el tratamiento de información (puestos de trabajo, memorias USB, discos duros, etc.)
- Personas que traten información.

- Instalaciones físicas en las que se ubiquen los activos de información.

Clasificación de los activos de información

Los activos de información primarios de NH deben clasificarse para determinar el nivel de protección a aplicar.

La clasificación de los activos de información primarios se debe realizar en función de los siguientes criterios:

- Disponibilidad: determina el impacto que provocaría la interrupción del acceso a la información en el momento en que se requiere.
- Confidencialidad e Integridad: determinada por la sensibilidad de la información y sus tratamientos.

En base a los citados criterios, se asignará un nivel de clasificación de disponibilidad (o nivel de disponibilidad) a un activo de información primario:

- Bajo: Cuando el responsable del proceso de negocio acepta que el tiempo objetivo de recuperación (RTO) igual o superior a veinticuatro (24) horas. Se entiende por RTO el tiempo que máximo aceptable para que el proceso de negocio o servicio esté parado desde que se produce un incidente hasta que se recupera (degradado, si es necesario); teniendo en cuenta los impactos legal, operacional, económico y en la imagen.
- Medio: Cuando el responsable del proceso de negocio acepta que el RTO igual o superior a una (1) hora e inferior a veinticuatro (24) horas.
- Alto: Cuando el responsable del proceso de negocio acepta que el RTO inferior a una (1) hora.

En base a los citados criterios, se asignará un nivel de clasificación de confidencialidad e integridad (o nivel de confidencialidad) a un activo de información primario:

- Publico: Información que no requiere de protección en su divulgación. Bien porque su divulgación, intencionada o accidental, no supone ningún tipo de impacto negativo para el Grupo NH; o bien porque la información es accesible por personas ajenas a NH a través de fuentes públicas.
- Uso interno: Información interna, necesaria para el correcto desempeño de NH. La información necesita protección, pero no está clasificada como Restringida o Confidencial. La divulgación, intencionada o accidental, de la cita información puede suponer un impacto económico leve al Grupo NH (más del 1% del presupuesto anual), un riesgo de sanción leve de acuerdo a las leyes o reglamentos, no deteriorando significativamente la imagen corporativa, no atentando contra los derechos de las personas físicas o jurídicas.
- Restringida: Información interna, exclusiva para determinados grupos de empleados, colaboradores, departamentos o áreas de negocio. Dicha información necesita protección, pero no está clasificada como Confidencial. La divulgación, intencionada o accidental, de la cita información puede suponer un impacto económico grave al Grupo NH (más del 5% del presupuesto anual), un riesgo de sanción grave de acuerdo a las leyes o reglamentos, deteriorando significativamente la imagen corporativa, o atentando directamente contra los derechos de las personas físicas o jurídicas.
- Confidencial: Información interna, exclusiva para grupos reducidos de empleados, colaboradores, departamentos o áreas de negocio. Dicha información necesita la máxima protección. La divulgación, intencionada o accidental, de la cita información puede suponer un impacto económico muy grave al Grupo NH (más del 10% de su presupuesto anual), un riesgo de sanción muy grave de acuerdo a las leyes o reglamentos, o deteriorando muy significativamente la imagen corporativa.

De manera general, en ausencia de clasificación de un activo de información se le aplicarán por defecto las medidas de seguridad requeridas para los activos clasificados con un nivel de disponibilidad Bajo y un nivel de confidencialidad Uso Interno.

Los niveles de clasificación de un activo de información primario se deben trasladar a los activos de información de soporte que intervengan en su tratamiento. Cuando un activo de información de soporte dé soporte a más de un activo de información primario, se deben heredar los niveles de clasificación más restrictivos.

Proceso de clasificación

La clasificación de los nuevos activos de información primarios se debe realizar de manera previa al inicio de un nuevo tratamiento.

El propietario de la información tiene que revisar la clasificación de los activos de información bajo su responsabilidad con una periodicidad anual o ante cualquier nuevo cambio que suponga una modificación en el tipo de información tratada, en el tratamiento de la información, en la finalidad de la información o en los actores implicados en el tratamiento. Como resultado de la citada revisión, se podrá:

- Modificar los niveles de clasificación asignados a un activo de información.
- Generar un nuevo activo de información con los niveles de clasificación diferentes a los del activo original a partir del cual se creó.

El propietario de la información tiene que informar a Information Security, así como al Delegado de Protección de Datos (DPD o DPO) del Grupo NH (o en su defecto a Legal Affairs), ante una nueva clasificación de un activo de información bajo su responsabilidad o ante un cambio en el nivel de clasificación de un activo.

Responsabilidades

En cada hotel o Departamento del Grupo NH, se debe designar a empleados que asuman el rol de propietarios de la información.

Los propietarios de la información son los responsables de asegurar que los activos de información de los cuales son responsables, se inventaríen y se clasifiquen de acuerdo a la Política de Seguridad de NH, así como los estándares normativos que emanan de la misma.

El propietario de la información puede delegar la tarea operativa de inventariar y clasificar un activo de información, pero no puede delegar sus responsabilidades en esta materia.

El propietario de la información es el responsable de informar a los empleados y colaboradores internos y externos de los niveles de clasificación de los activos de información que tratan por razón de sus funciones y responsabilidades.

Asimismo, Information Security es el responsable de informar a IT & Systems de los niveles de clasificación de los activos de información que tratan por razón de sus funciones y responsabilidades.

La aplicación de medidas de seguridad organizativas y técnicas por parte de los empleados y colaboradores internos y externos de NH debe atender, entre otras razones, a los niveles de clasificación asignados en los

activos de información. Las citadas medidas de seguridad se encuentran detalladas en la Política de Seguridad de NH, así como los estándares normativos que emanan de la misma.

5.3.3. Manipulación de los soportes

Etiquetado de soportes

Los soportes de información (entre otros, documentación en papel, ordenadores portátiles, memorias USB, discos duros externos, CDs, DVDs, etc.) del Grupo NH se deben etiquetar de forma que se indique visible y claramente el nivel de confidencialidad del activo de información contenido de clasificación más restrictivo.

En los soportes digitales, se debe etiquetar la información mediante el uso de marcas de agua donde se indique el nivel de clasificación del documento y a través de texto insertado en la cabecera de página de los documentos.

En los soportes físicos, se debe etiquetar la información a través de etiquetas o inscripciones en las que se indique el nivel de clasificación de la información.

Manipulación de soportes

La información clasificada con un nivel de confidencialidad Uso Interno o superior debe ser accesible y tratable únicamente por los empleados y colaboradores internos y externos autorizados para ello. Por ello, los soportes que contengan información clasificada deben custodiarse y almacenarse para evitar accesos no autorizados.

Los soportes que el Grupo NH custodie en el marco de un contrato o acuerdo legal, deben ser protegidos de acuerdo con los términos especificados en dicho contrato o acuerdo.

Los empleados y colaboradores internos y externos deben cumplir con los criterios de archivo establecidos en el Grupo NH.

Distribución

Salvo autorización previa del propietario de la información, los empleados y colaboradores internos y externos no deben extraer o compartir información clasificada con un nivel de confidencialidad Uso Interno o superior fuera de las instalaciones del Grupo NH, con independencia del soporte en el que se encuentre.

El propietario de la información debe autorizar exclusivamente los casos en que el transporte o distribución sea inevitable para el buen funcionamiento de los procesos de negocio de NH.

En los casos en que el propietario de la información lo haya autorizado, el empleado o colaborador interno o externo que vaya a custodiar el soporte durante el transporte debe tener en cuenta los siguientes aspectos:

- Los soportes deben estar asegurados durante todo el transporte.
- De manera previa a la entrega de un soporte etiquetado como Restringida o Confidencial, se debe confirmar la identidad del receptor.
- Los soportes etiquetados como Confidencial deben poder ser rastreados desde su distribución hasta su recepción.

De manera general, no se debe enviar o transmitir datos técnicos y copias de software a otros países o estados. En caso de que sea inevitable para el buen funcionamiento de los procesos de negocio de NH, se debe consultar previamente a Legal Affairs para confirmar que no se incumplirían normativas de importación/exportación, ni leyes o regulaciones de propiedad industrial o intelectual.

Impresión

Los empleados y colaboradores internos y externos que impriman información clasificada como Uso Interno, Restringida o Confidencial deben hacer todos los esfuerzos razonables para asegurar que los soportes permanecen seguros durante todo el ciclo de vida de la impresión. Esto incluye, pero no se limita:

- Imprimir información clasificada como Restringida o Confidencial en impresoras que se encuentren situadas en el área de visión del usuario.
- No abandonar documentos en fotocopiadores, escáneres, impresoras o faxes.
- Eliminar de manera segura documentos que no sean necesarios.
- Evitar generar y acumular de manera innecesaria documentación impresa. En la medida de lo posible, trata la información en formato digital.

Copia

Los empleados y colaboradores internos y externos deben tener en cuenta los siguientes aspectos cuando copien soportes con información de NH:

- Los soportes que contengan información clasificada como Restringida o Confidencial sólo se pueden copiar con el permiso del propietario de la información.
- Las copias de soportes deben clasificarse por defecto con los mismos niveles de clasificación que el soporte original.

Almacenamiento

Con respecto al almacenamiento físico de soportes que contengan información titularidad o bajo la responsabilidad de NH, los empleados y colaboradores internos y externos deben tener en cuenta los siguientes aspectos:

- Los soportes que contengan información clasificada como Restringida o Confidencial deben almacenarse en una habitación cerrada con llave o, en su defecto, dentro de un archivador con llave o caja fuerte.
- Los soportes que contengan información clasificada como Restringida o Confidencial deben almacenarse en un área restringida (es decir, área no pública).
- Los empleados y colaboradores internos y externos deben seguir una política de mesas limpias, es decir, se debe:
    - Se debe evitar descuidar soportes encima de mesas o estanterías al finalizar la jornada laboral o ante una ausencia prolongada
    - No se deben almacenar soportes en áreas públicas
    - En las salas de reuniones no deben descuidarse soportes, asimismo se deben borrar pizarras, *flip charts* o similares al abandonar la sala

- Las habitaciones donde se almacenan soportes, deben quedar con la puerta cerrada al finalizar la jornada laboral o ante una larga ausencia

En relación con el almacenamiento digital, en aquellos casos en que el soporte informático sea extraíble y contenga información clasificada con un nivel de confidencialidad Restringida o Confidencial, los datos almacenados en el mismo deben ser cifrados durante el almacenamiento.

Borrado seguro

Los empleados y colaboradores internos y externos deben destruir de manera segura la documentación en papel que no sea necesaria. De manera general, se debe hacer uso de papeleras de seguridad para información confidencial o de destructoras de papel de NH. Está expresamente prohibida depositar los soportes en papeleras (sin protección) y la reutilización de documentación en papel con información sensible de NH.

Asimismo, los soportes de información se deben destruir o borrar de manera segura cuando ya no sea necesario retener la información por motivos comerciales o legales.

5.4. CONTROL DE ACCESO

5.4.1. Requisitos de negocio para el control de acceso

Los empleados y colaboradores internos y externos deben acceder exclusivamente a la información, sistemas de información y servicios de TI de NH necesarios para el desempeño de sus funciones y responsabilidades en el Grupo NH.

Los permisos de acceso deben otorgarse teniendo en cuenta el principio de necesidad de conocimiento, asegurando que los empleados y colaboradores internos y externos acceden a los datos de los sistemas y servicios de TI necesarios para el desarrollo de sus tareas y únicamente durante el periodo de tiempo necesario para ello. Asimismo, los permisos de acceso siempre deben asignarse siguiendo el principio de mínimos privilegios, es decir: todo lo que no está permitido, está prohibido.

5.4.2. Gestión de acceso de usuario

Identificación

Por defecto, las cuentas de usuario son nominativas. Es decir, existe una relación unívoca entre una cuenta de usuario y la persona responsable de la misma. Queda prohibido el uso de cuentas genéricas. La creación de este tipo de cuentas debe ser autorizada por Information Security, y se mantendrá un registro de dichas excepciones.

En lo que respecta al patrón de construcción del identificador de usuario, se definirán diferentes patrones en función de las tipologías de usuarios existentes en los sistemas (p.e., personal de hoteles, colaboradores

externos, personal de IT & Systems, etc.) El objetivo de facilitar las labores de administración de usuarios y disminuir la probabilidad de que se produzcan errores.

Asignación de privilegios

La asignación de los privilegios y permisos debe estar controlada y restringida. Para ello se deben de tener en consideración los siguientes aspectos:

- Principio de mínimo privilegio: se debe asignar a los usuarios el perfil correspondiente a su puesto de trabajo, que debe contener los mínimos privilegios para el desempeño de sus funciones.
  No se debe crear ninguna cuenta de usuario ni se deben otorgar privilegios de acceso hasta que no se haya completado el proceso de autorización.
- Control de acceso basado en roles: la asignación de privilegios se debe realizar a partir de roles que se asocien al puesto de trabajo de los usuarios. La definición de roles debe tener en cuenta los aspectos:
  - Granularidad: se permite la posibilidad de permitir diferentes niveles de acceso.
  - Segregación de funciones: permite identificar y evitar la asignación simultánea de privilegios a un usuario de forma que se reduzca el riesgo de uso indebido en la gestión o realización de ciertas funciones o áreas de responsabilidad.

Alta, baja y modificación de permisos de acceso

People (Recursos Humanos) del Grupo NH es el responsable de iniciar un proceso de alta o baja de permisos de acceso para empleados internos. Asimismo, el responsable del afecta es el responsable de iniciar un proceso de modificación de permisos de acceso para empleados internos.

En el caso de altas, bajas o modificaciones de permisos de acceso para colaboradores externos, el responsable de iniciar la solicitud es el responsable del proveedor en el Grupo NH, el cual es personal interno de NH.

Al inicio de la tramitación de una solicitud de alta, baja o modificación de los permisos de acceso, se debe verificar la identidad del solicitante y su nivel de atribución, para comprobar que la petición la realiza el personal autorizado.

Una vez la solicitud inicial ha sido aprobada, el proceso de gestión de usuarios consta de las siguientes fases:

- Alta: la creación del usuario en los repositorios correspondientes será realizada, preferentemente, de forma automática, a partir de la información disponible en las fuentes de autorización. En la creación de usuarios con fecha de vigencia conocida (contratos temporales, personal externo, etc.) y siempre que el sistema lo permita, se establece la fecha de expiración automática de dicho usuario.
- Baja: baja o bloqueo del usuario en la aplicación. Del mismo modo que en las altas, la baja se realizará mediante procesos automatizados, siempre que sea posible. Si se prevé que el motivo por el que se produce un cese puede dar lugar a una situación conflictiva, el inicio de la solicitud de la baja de las cuentas de usuario se realiza con antelación a la comunicación formal de la baja al trabajador, indicando su efecto inmediato.
- Modificación: La modificación de los privilegios de un usuario se puede realizar de dos modos:

- La modificación de los roles asignados a un puesto de trabajo. Por defecto, se tratará de canalizar todas las modificaciones de privilegios en las aplicaciones mediante el mantenimiento del modelo de roles.
- La asignación singular de privilegios a dicho usuario.

Todas las acciones llevadas a cabo asociadas al proceso de gestión de usuarios y privilegios deberán quedar registradas, con el fin de tener un histórico de las peticiones atendidas y servir como soporte para las revisiones periódicas. Asimismo, Information Security coordinará periódicamente la ejecución de revisiones del proceso de asignación de usuarios y privilegios en los sistemas de información y servicios de TI de NH.

5.4.3. Responsabilidades

Las credenciales de acceso generadas por NH, son propiedad del Grupo NH.

Los empleados y colaboradores internos y externos deben mantener las contraseñas y códigos de acceso en secreto, incluso hasta cuando otro empleado o colaborador lo solicite.

Las credenciales de acceso son de uso exclusivo del empleado o colaborador al cual pertenecen. Al tratarse de información confidencial, las credenciales deben almacenarse acorde al nivel de clasificación establecido. Asimismo, los empleados y colaboradores internos y externos deben modificar las contraseñas siempre que éstas sean comprometidas o exista sospecha de ello.

5.4.4. Control de acceso a sistemas y aplicaciones

Todos los sistemas de información y servicios de TI de NH deben evitar el acceso a la información del Grupo NH si el usuario o el proceso no se ha identificado y autenticado previamente.

Autenticación

De manera general, la validación de la identidad de los usuarios en los sistemas de información de NH se realiza mediante la combinación del identificador de usuario y la contraseña. Para ello, el control de acceso a sistemas de información y servicios de TI que traten información de NH debe cumplir con los siguientes aspectos:

- Obligación de cambio periódico de la contraseña, código secreto o similar, y posibilidad de cambiarla en cualquier momento por parte de los usuarios de las aplicaciones.
  De manera general, las contraseñas deberán ser modificadas cada sesenta (60) días como máximo.
- Obligación de construir contraseñas complejas: de una longitud mínima, que incluyan diferente tipología de caracteres (mayúsculas, minúsculas, números, caracteres especiales, etc.), palabras reservadas, etc.
  De manera general, las contraseñas deben tener una longitud mínima de seis (6) caracteres, los cuales deberán contener caracteres alfanuméricos combinando mayúsculas y minúsculas.
- Bloqueo de la cuenta de usuario tras superar los cinco (5) intentos de acceso fallidos.
- Imposibilidad de repetir las últimas contraseñas utilizadas.

De manera general, se debe impedir utilizar de nuevo cualquiera de las tres (3) últimas contraseñas previas.

- Obligación de generar de forma aleatoria una primera contraseña temporal para el acceso a la aplicación y, tras el primer inicio de sesión exitoso, exigir su cambio.
- Delegar, en la medida de lo posible, la gestión del proceso de autenticación en los repositorios corporativos de usuarios del Grupo NH, evitando así el uso de repositorios propios de cada aplicación.
- No almacenar contraseñas en claro en repositorios de autenticación, código fuente o scripts.

En el caso de las cuentas de usuarios sin privilegios utilizadas en entornos, sistemas y servicios que procesen datos de medios de pagos (p.e., números de cuenta, números de tarjetas bancarias, nombres de titulares, códigos de servicio, fechas de vencimientos, etc.) deben tener una longitud mínima de siete (7) caracteres y se debe impedir utilizar de nuevo las cuatro (4) últimas contraseñas previas.

En el caso de las cuentas con privilegios de administración y de las cuentas genéricas, las contraseñas deben tener una longitud mínima de doce (12) caracteres y deberán cambiarse como máximo cada treinta (30) días.

Cualquier excepción que suponga la aplicación de una política de autenticación menos robusta que la definida anteriormente debe ser autorizada por Information Security, y se mantendrá un registro de dichas excepciones.

Procedimientos seguros de inicio de sesión

El acceso a la información y sistemas de información de NH debe controlarse por medio de un procedimiento seguro de inicio de sesión. Dicho procedimiento debe asegurar que las contraseñas, códigos secretos o similares no se muestren durante el proceso de inicio de sesión.

En función de los riesgos y de los niveles de clasificación de la información, se considerará la autenticación de doble factor. Este método de autenticación combina dos de los siguientes tres factores:

- Factor de conocimiento: algo que el usuario **sabe** (p.e., contraseñas, códigos secretos, etc.)
- Factor de propiedad: algo que el usuario **tiene** (p.e., dispositivo, tarjeta de acceso, etc.)
- Factor inherente: algo que el usuario **es** (p.e., huella dactilar, iris, etc.)

Para el acceso remoto desde fuera de las redes internas del Grupo NH a cualquier sistema de información o servicio de TI donde se trate información de medios de pago (p.e., números de cuenta, números de tarjetas bancarias, nombres de titulares, códigos de servicio, fechas de vencimientos, etc.), así como el acceso en remoto de tareas de administración a los citados sistemas y servicios, se debe utilizar doble factor de autenticación.

Trazabilidad

En los sistemas de información y servicios de TI donde se trate información de NH se deben generar registros (*logs*) que permiten la trazabilidad de las acciones realizadas.

Information Security podrá colaborar en la definición de los requisitos en cuanto a generación de registros por parte de los sistemas y servicios, como parte de su colaboración en el ciclo de vida de desarrollo de aplicaciones.

No obstante, lo anterior, el Responsable del Proyecto debe indicar, durante la etapa de definición de requerimientos:

- Transacciones a registrar.
- Tiempo de almacenamiento de las trazas.
- Procedimiento de explotación de los registros: bajo petición, ante la sospecha de incidentes de seguridad o periódicamente.
- Requisitos adicionales impuestos por algún requisito normativos específicos (p.e., PCI DSS, leyes y regulaciones en materia de protección de datos personales, etc.)

5.5. CRIPTOGRAFÍA

5.5.1. Implementación y uso de la criptografía

Métodos criptográficos

La decisión sobre el uso de métodos criptográficos tiene que estar basada en los niveles de clasificación de la información.

En referencia al cifrado de la información se deben tener en cuenta los siguientes aspectos:

- La información clasificada como Confidencial debe almacenarse siempre cifrada.
- Las transferencias de información clasificada como Restringida o Confidencial a las DMZ o redes públicas (p.e., Internet) deben cifrarse.
- La información clasificada como Confidencial que contenga medios de pago (p.e., números de cuenta, números de tarjetas bancarias, nombres de titulares, códigos de servicio, fechas de vencimientos, etc.) debe ir cifrada también en las comunicaciones entre sistemas de información en las redes internas de NH.

Selección de métodos criptográficos

Sólo deben utilizarse métodos criptográficos cuya seguridad y fortaleza hayan sido previamente evaluadas por expertos. Principalmente, se debe tener en cuenta el estado del arte del algoritmo criptográfico a utilizar y la longitud de clave.

Sólo se deben utilizar métodos criptográficos que estén documentados y sean accesibles al público.

Para todos los sistemas y aplicaciones que soportan medios de pago, no debe utilizarse ningún algoritmo criptográfico o protocolo débil.

Para garantizar una protección robusta, se pueden aplicar diferentes métodos criptográficos:

- Confidencialidad:
  - Criptografía simétrica (p.e., AES)
  - Criptografía asimétrica (p.e., RSA)

  - Criptografía híbrida (p.e., RSA junto con AES)
- Integridad:
  - Algoritmos Hash (p.e., SHA-2) junto con firmas asimétricas (p.e., RSA)
  - Códigos de autenticación de mensaje (MAC)
- No repudio:
  - Contraseñas
  - One Time Passwords (OTP)
  - Firmas asimétricas
  - Métodos biométricos (p.e., huellas dactilares, reconocimiento de iris)

Asimismo, los métodos criptográficos pueden utilizarse en diferentes capas del modelo OSI:

- Nivel 3: Capa de red (IPSEC)
- Nivel 6: Capa de presentación (TLS)
- Nivel 7: Capa de aplicación (S/MIME)

A continuación, se listan algoritmos y protocolos seguros:

- Algoritmos de cifrado simétrico:
  - AES (con longitud de clave mínima de) 256 (bits)
  - Triple DES 168
  - RC5 256
  - RC6 256
  - Twofish 256
  - IDEA 128
- Algoritmos de hash:
  - SHA-2 256
  - SHA-2 512
  - Whirlpool 512
- Algoritmos de cifrado asimétrico:
  - RSA 4096
  - Ed25519
- Protocolos criptográficos:
  - TLSv1.2
  - WPA2
  - SSHv2
  - L2TP/IPsec

Un producto criptográfico es un producto que implementa métodos criptográficos. De forma previa a la adquisición de un producto criptográfico, se deben tener en cuenta los siguientes criterios:

- El producto debe haber sido certificado (p.e., acorde con los requerimientos de FIPS) por un experto independiente.
- Los productos criptográficos deben caracterizarse por su facilidad de uso para así evitar errores durante la administración y utilización del producto.

- Debe decidirse si las medidas criptográficas se implementan a nivel de hardware, firmware o software. Esta decisión debe tomarla Information Security.
- Se deben seleccionar preferiblemente productos europeos frente a productos de fabricantes extranjeros.

Disponibilidad y compatibilidad

Cuando se utilicen métodos criptográficos, es importante asegurar la disponibilidad del servicio, especialmente, cuando el uso de algoritmos criptográficos fuertes pueda provocar problemas de compatibilidad en los sistemas.

Cuando se usen métodos criptográficos, se debe comprobar que los productos utilizados son compatibles con la mayoría de estándares y la migración a otro producto o a otro proveedor no implica grandes esfuerzos o complicaciones.

Por todo ello, es importante realizar las migraciones a algoritmos criptográficos fuertes en entornos de prueba antes de su implementación en el entorno de producción.

Rentabilidad

Además de los gastos derivados de la implantación de los métodos criptográficos (licencias de productos, costo de implementación e integración), se deben tener en cuenta costes operativos:

- Cursos de formación
- Soporte técnico
- Mantenimiento
- Recursos adicionales (p.e., CPU)

Influencias de otros mecanismos de seguridad

El cifrado de datos y el establecimiento de canales cifrados pueden tener un efecto negativo en la seguridad, por ejemplo, en la protección contra el malware. Por esta razón, es necesario involucrar a Information Security con el objetivo de realizar una evaluación de riesgos, y si es necesario, implementar controles compensatorios. Por ejemplo:

- Los sistemas de detección de intrusos (IDS) y los sistemas de prevención de intrusos (IPS) no pueden detectar patrones en tráfico cifrado. Por esta razón, se deben utilizar módulos de inspección de tráfico TLS.
- Los sistemas de filtrado de contenido web deben ser capaces de inspeccionar tráfico cifrado.

Las claves de descifrado no deben estar asociadas con cuentas de usuario. Éstas deben estar accesibles a la menor cantidad de custodios necesarios. Asimismo, se debe definir un período de cifrado asociado a cada clave, debiendo ser destruidas cuando ya no sean necesarias.

Uso de productos criptográficos

Los empleados y colaboradores internos y externos que operen o implementen productos criptográficos, deben recibir formación especializada sobre cómo gestionar el producto. Estos empleados deben conocer el uso y los

beneficios de los diferentes métodos criptográficos y tener una visión general de los conceptos básicos de la criptografía.

Si ocurre un incidente de seguridad relacionado con un producto criptográfico, Information Security debe ser informada de forma inmediata. Por lo tanto, es importante que los operadores e implementadores conozcan los procedimientos de gestión de incidentes de seguridad.

Los productos criptográficos deben configurarse de la forma más segura posible, impidiendo que un usuario pueda eludir fácilmente las medidas de seguridad.

5.5.2. Gestión de claves

La administración, transmisión, almacenamiento y actualización de claves criptográficas se debe realizar de manera segura, de acuerdo con los siguientes principios:

- Las soluciones de cifrado deben generar claves sólidas.
- Las soluciones de cifrado deben distribuir las claves de forma segura, es decir, sólo se entregan a los custodios identificados y nunca se distribuyen en texto claro.
- Los custodios de claves criptográficas deben declarar formalmente que han comprendido y aceptan sus responsabilidades como custodios de claves.
- Las soluciones de cifrado deben almacenarse de forma segura (p.e., cifrando las claves con una clave de cifrado de claves).
- Se debe definir un período de cifrado para cada tipo de clave utilizada, en base al algoritmo subyacente, tamaño y longitud de la clave, peligro de riesgo de la clave y la confidencialidad de los datos cifrados. Al finalizar el citado período, las claves deben cambiarse.
- Las soluciones de cifrado deben proporcionar un proceso para el reemplazo de claves.
- Las claves que ya no se utilicen o necesiten, o las que se sospeche que pueden haber sido comprometidas, se deben anular o destruir de manera segura.
- El conocimiento dividido y control doble de claves se debe utilizar en las operaciones manuales de administración de claves.
- Las soluciones de cifrado no deben permitir la sustitución de claves por parte de fuentes no autorizadas.

5.5.3. Gestión de certificados

La administración de los certificados electrónicos se debe realizar de manera segura, dando cumplimiento a los siguientes aspectos:

- El proceso de validación de certificados debe confirmar que no están revocados, ni caducados. Asimismo, en dicho proceso también se debe confirmar que está firmado por una Autoridad de Certificación (CA) de confianza.
- La implementación y utilización de una CA interna debe ser aprobada por Information Security.

- Ante la necesidad de usar certificados externos en sistemas de información, servicios de TI o para usuarios, se deben notificar a Information Security de dicha necesidad.
- No se deben instalar certificados emitidos por CA externas en puestos de empleados y colaboradores internos y externos.

5.6. SEGURIDAD FÍSICA Y DEL ENTORNO

5.6.1. Áreas seguras

Tipologías de áreas

NH ha implantado una serie de mecanismos para garantizar la seguridad de las instalaciones en las que se encuentran ubicados y/o se tratan sus activos de información.

En concreto, a la hora de considerar las medidas de seguridad física a implantar, cabe diferenciar tres tipos de ubicaciones:

- Áreas públicas: Comprenden aquellas salas, oficinas o similares de libre acceso para los clientes de NH. Principalmente, estas áreas están ubicadas en los hoteles del Grupo NH.

- Áreas de trabajo: Comprenden aquellas salas, oficinas o similares, con independencia de su ubicación, en las cuales se almacene o custodie información del Grupo NH y sean de acceso exclusivo para empleados y colaboradores internos y externos de NH. Deben ser clasificadas como áreas de trabajo los despachos en hoteles, los archivos de documentación y las oficinas en las que se encuentra empleados del Grupo NH.

- Áreas técnicas: Comprenden aquellas salas donde se encuentra el equipamiento informático y de comunicaciones, excluyendo los puestos de trabajo. Es decir, son las ubicaciones dónde se encuentran centros de procesamiento de datos, cuartos de comunicaciones, etc. Estas zonas deben ser de acceso exclusivo para empleados y colaboradores internos y externos de NH previamente autorizados.

Cabe destacar que dichas áreas pueden estar ubicadas en instalaciones propias del Grupo NH o en instalaciones de terceros en los que se hayan externalizado ciertos servicios. En cualquier caso, e independientemente de la ubicación, se deben aplicar medidas de seguridad equivalentes a las detalladas en la Política de Seguridad de NH, así como los estándares normativos que emanan de la misma.

Medidas de seguridad

NH ha implantado diferentes medidas de seguridad física en función de la tipología de ubicaciones desde las que se tratan activos de información, en función del nivel de riesgo a los que se encuentran sometidos cada tipología, determinado a partir de las siguientes variables:

- Activos de información ubicados o tratados, valorando el impacto que supondría su pérdida o daño.

- Nivel de exposición frente a potenciales amenazas, de acuerdo al nivel de accesibilidad al lugar, el aislamiento de éste con respecto a otras zonas de la instalación o respecto al perímetro exterior, frecuencia de acceso de colaboradores externos, etc.

Los mecanismos de seguridad física implantados en cada una de las ubicaciones pueden ser clasificados en las siguientes categorías:

- Control de acceso físico, correspondiente a las medidas establecidas para prevenir y detectar accesos no autorizados.
- Sistemas de detección volumétrica.
- Sistemas de circuito cerrado de televisión (CCTV).
- Vigilancia física, mediante vigilantes de seguridad.
- Seguridad ambiental, que engloba los mecanismos de protección medioambiental y amenazas de carácter externo y del entorno.

La definición de las medidas de protección a aplicar en las áreas públicas, de trabajo y técnicas es responsabilidad de Operations.

Áreas públicas

En las áreas públicas se deben implantar las medidas de seguridad necesarias y proporcionales para garantizar un control de acceso físico a los equipos, dispositivos y soportes que contengan información de NH.

Los empleados y colaboradores internos y externos deben custodiar adecuadamente todos los soportes que contengan información de NH bajo su responsabilidad, especialmente en las áreas públicas de las instalaciones del Grupo NH.

Áreas de trabajo

En las áreas de trabajo se deben implantar medidas de seguridad para prevenir el acceso no autorizado a equipos, dispositivos, soportes y a las redes internas de NH. Entre otras, se deben implantar:

- Mecanismos de identificación de empleados y colaboradores internos y externos de NH (p.e., tarjetas de acceso, sensores biométricos, etc.)
- Mecanismos de identificación utilizados por las visitas, los cuales deben poder permitir diferenciar de forma clara respecto a los empleados y colaboradores internos y externos de NH.
- Revisión periódica de permisos de acceso físico.
- Mecanismos que limiten el acceso físico (p.e., puertas con llave, control mediante código, lectores de tarjetas de acceso, controles biométricos, etc.)
- Uso de dispositivos de almacenamiento seguro (p.e., armarios cerrados con llave para el almacenamiento de documentación y soportes, etc.)

Para las áreas de trabajo que por cualquier motivo presenten riesgos específicos, se puede considerar la implantación de medidas de seguridad adicionales. En este sentido, se contempla el uso de las siguientes medidas:

- Implantación de sistemas de video-vigilancia. De manera general, las grabaciones de estos sistemas deben ser almacenadas durante menos de treinta y un (31) días, a menos que otra ley o reglamento vigente disponga un periodo de retención inferior.
- Instalación de puertas dotadas de cerraduras eléctricas.
- Sensores volumétricos.
- Vigilantes de seguridad.

Áreas técnicas

A nivel de zonas técnicas, se distinguen dos tipos de instalaciones:

- Centros de Proceso de Datos (CPD).
- Salas reducidas de infraestructura de sistemas y comunicaciones (p.e., armarios de comunicaciones, sala de comunicaciones, salas de servidores, etc.)

En relación con los CPD:

- Mecanismos de identificación de empleados y colaboradores internos y externos de NH (p.e., tarjetas de acceso, sensores biométricos, etc.)
- Mecanismos de identificación utilizados por las visitas, los cuales deben poder permitir diferenciar de forma clara respecto a los empleados y colaboradores internos y externos de NH.
- Procedimientos para que las visitas vayan acompañadas en todo momento.
- Revisión periódica de permisos de acceso físico.
- Implantación de registro de los intentos de acceso (tanto los autorizados como los denegados).
- Mecanismos que limiten el acceso físico (p.e., puertas con llave, control mediante código, lectores de tarjetas de acceso, controles biométricos, etc.)
- Uso de dispositivos de almacenamiento seguro específicos para servidores y dispositivos de comunicaciones (p.e., RACK con llave)
- Implantación de protecciones o dispositivos que palien la falta de suministro eléctrico (p.e., SAI, grupos electrógenos, etc.).
- Implantación de sistemas de iluminación de emergencia para el caso en el que falle completamente el suministro eléctrico.
- Implantación de sistemas de video-vigilancia que graven de manera ininterrumpida durante 24 horas al día. De manera general, las grabaciones de estos sistemas deben ser almacenadas durante menos de treinta y un (31) días, a menos que otra ley o reglamento vigente disponga un periodo de retención inferior.
- Sensores volumétricos.
- Vigilantes de seguridad.
- Implantación de sistemas contra incendios, de acuerdo con las leyes y reglamentos vigentes.
- Medidas medioambientales necesarias para garantizar el buen funcionamiento y estado de los equipos, dispositivos y soportes.
- Sistema de monitorización de las condiciones medioambientales, como mínimo de temperatura y humedad.
- Medidas de eficiencia energética.

En cuanto a las salas reducidas de infraestructura de sistemas y comunicaciones, se debe disponer de mecanismos que limiten el acceso físico a las mismas (p.e., uso de puertas con cerradura, armarios con llave, control mediante código, etc.) y las medidas medioambientales necesarias para garantizar el buen funcionamiento y estado de los equipos, dispositivos y soportes.

5.6.2. Seguridad de los equipos

Emplazamiento y protección

En las áreas públicas, los empleados y colaboradores internos y externos no deben ubicar los mismos al alcance de terceros, como clientes o visitantes, a fin de evitar sustracciones o manipulaciones. Se debe prestar especial atención a evitar que los conectores de los equipos, donde se pueden conectar memorias USB, no estén ubicadas al alcance de terceros.

Los equipos y dispositivos que traten o contengan información de NH, ya sean informáticos o documentación en papel, deben estar almacenados en áreas de trabajo o áreas técnicas, a las cuales únicamente pueda acceder personal debidamente autorizado.

Los equipos y dispositivos deben protegerse ante cualquier problema que pueda causar fallos en las utilidades de soporte (p.e., fallos en el suministro eléctrico o en la ventilación). Para una adecuada gestión de las utilidades de soporte, se debe:

- Cumplir con las especificaciones del fabricante de equipamiento.
- Monitorizar fallos en el funcionamiento.
- Tener redundancia de enlaces eléctricos.
- El equipamiento de comunicaciones debe estar conectado al menos a dos enlaces de comunicaciones de distintos proveedores.
- Asegurar el suministro de agua que provee a los sistemas de aire acondicionado.

Además de esto, las utilidades de soporte deben inspeccionarse periódicamente para asegurar su correcto funcionamiento y reducir el riesgo de fallo.

Seguridad en el cableado

El cableado de comunicaciones y energía debe protegerse a fin de evitar posibles pérdidas de datos, intercepciones o daños. Los siguientes requisitos deben considerarse:

- Las líneas de telecomunicaciones y de transporte de energía eléctrica deben estar protegidas físicamente (p.e., con tubos, canales, etc.) o ir bajo tierra.
- Las redundancias de acometidas, tanto eléctricas como de telecomunicaciones, no deben compartir la misma ubicación, ni conducto de acceso al edificio.
- Los cables eléctricos deben estar separados de los cables de telecomunicaciones para evitar interferencias y posibles daños.
- Los cables deben estar correctamente identificados y etiquetados para evitar errores en la manipulación de los mismos.

Mantenimiento

El correcto mantenimiento de los equipos y dispositivos debe llevarse a cabo con el objetivo de evitar posibles fallos y garantizar así su disponibilidad. Los siguientes requisitos deben tenerse en cuenta:

- Sólo los empleados y colaboradores internos y externos autorizados pueden llevar a cabo tareas de mantenimiento e inspección sobre el equipamiento.
- En caso de retirada de un equipamiento por avería, debe sustituirse lo antes posible para continuar con el desarrollo de los procesos de negocio del Grupo NH.
- Las tareas de mantenimiento deben realizarse siguiendo las especificaciones recomendadas por los fabricantes.

Retirada de equipos

Los equipos, dispositivos, software u otro activo de información no deben ser retirados sin previa autorización. Para evitar que el equipamiento sea retirado sin autorización, los siguientes requisitos deben considerarse:

- Los empleados y colaboradores internos y externos que estén autorizados para retirar equipamiento, deben estar claramente identificados.
- Debe quedar registrado cuando se retira un activo de información y cuando es devuelto a su lugar de origen.

Antes de reutilizar o retirar el equipamiento, se debe haber destruido o borrado toda la información contenida en el mismo, utilizando técnicas que impidan recuperar la información, en vez de utilizar las opciones de borrado estándar que no sobrescriben la memoria.

5.7. SEGURIDAD DE LAS OPERACIONES

5.7.1. Procedimientos y responsabilidades operacionales

Documentación de procedimientos de operación

Los procedimientos relacionados con la operación y administración de los sistemas de información se encuentran formalizados y están disponibles para todos aquellos usuarios que los necesiten para llevar a cabo las funciones de su puesto de trabajo.

Gestión de cambios

Se define como cambio operacional aquellos realizados en los sistemas, servicios, equipos o procedimientos que afecten a las instalaciones y a los sistemas de información y servicios de TI de NH que se encuentran en entornos productivos.

Durante la gestión de cambios, se deben determinar los siguientes principios:

- Identificar los sistemas de información de NH que pueden verse directa o indirectamente impactados por el cambio.

- Evaluar el impacto que puede ocasionar la aplicación del cambio ante una posible pérdida de integridad, confidencialidad o disponibilidad de la información.
- Realizar un análisis de riesgos que permita identificar y gestionar los riesgos asociados a dicho cambio.
- Desarrollar un plan de retorno (*roll-back*) que permita recuperar el estado previo a la implantación del cambio.

Con anterioridad a la implantación de los cambios en los entornos de producción, se debe probar previamente la efectividad de los cambios aplicados en un entorno controlado de pruebas, verificando la correcta implantación del mismo.

Todos los cambios que afecten a los sistemas, aplicaciones y datos del entorno de producción de NH debe estar aprobado y autorizado previamente por un Comité de Cambios. Asimismo, los cambios operacionales deben ser identificados y registrados, quedando dicho registro disponible para su revisión en caso de ser necesario. En este registro se debe incluir el alcance de los cambios, sistemas afectados por la implantación del cambio, fallos ocurridos y los procesos de recuperación.

Gestión de capacidades

El proceso de gestión de capacidades permite planificar el dimensionamiento de los recursos tecnológicos y humanos necesarios para garantizar las necesidades de negocio. Las capacidades de los recursos tecnológicos y humanos deben ser monitorizadas de manera continua para poder realizar un dimensionamiento adecuado y adelantarse a posibles saturaciones futuras.

Para ello, se debe establecer indicadores clave (p.e., estadísticas de utilización de CPU, memoria, espacio de discos, etc.) que permitan mantener un seguimiento de los recursos tecnológicos del Grupo NH. Dichos indicadores deben permitir monitorizar de manera continua los recursos y sistemas de información de NH y analizar las causas que puedan provocar un exceso o defecto de la capacidad planificada inicialmente, con el objetivo de adecuar los mismos y garantizar los requerimientos establecidos.

Asimismo, es necesario identificar los sistemas más críticos para el negocio, los cuales serán los más prioritarios para determinar las actuaciones inmediatas que permitan asegurar el correcto dimensionamiento de los recursos en base a las necesidades del Grupo NH.

Separación de los recursos de desarrollo, prueba y operación

Los entornos productivos y no productivos deben permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional. Esta separación de entornos es importante para el negocio del Grupo NH, debido al control de seguridad adicional que supone.

Para favorecer una adecuada segregación de funciones durante el ciclo de vida de desarrollo de una aplicación o sistema, los entornos se clasifican en las siguientes tipologías:

- Entornos no productivos:
  - Entorno de desarrollo: orientado al personal de desarrollo para la programación de sus proyectos. Los desarrollos tienen lugar en este entorno controlado, que no afecta al trabajo normal de NH. Se debe trabajar con una muestra modificada de los datos, así como con programas y procesos que sean copias de los de producción, donde el programador no puede alterar la información de aquel entorno y los cambios en éste no tengan consecuencias.

- Entorno de pruebas: entorno opcional creado en función de las necesidades del proyecto. En dicho entorno se realizan las pruebas unitarias que permiten verificar el correcto funcionamiento de las funcionalidades implementadas en el entorno de desarrollo. Dicho entorno no puede ser modificado por el analista o programador, quien debe retornar al entorno de desarrollo si debe hacer nuevos cambios a los procesos.
- Entorno de integración: entorno opcional donde se realizan las pruebas de sistema, de estrés, de integración, de usuario, etc. Este entorno debe simular a los entornos productivos, de manera que las pruebas realizadas en el mismo sean lo más verídicas posible. Asimismo, en este entorno se puede verificar la interacción con otras aplicaciones o sistemas. Dicho entorno no puede ser modificado por el analista o programador, quien debe retornar al entorno de desarrollo si debe hacer nuevos cambios a los procesos. En este entorno se trabaja con una muestra de la información más completa que en los entornos anteriores.

- Entornos productivos: en estos entornos se ejecutan los procesos reales de NH. Son entornos donde no caben realizar pruebas de ningún tipo, ya que cualquier error puede tener graves consecuencias para NH de resultado inmediato. Toda actividad realizada sobre los mismos debe quedar convenientemente registrada y se debe revisar periódicamente.

5.7.2. Protección contra el software malicioso (malware)

Cualquier sistema de información de NH es potencialmente a vulnerable a *software* malicioso (*malware*). Las consecuencias de una infección en los sistemas de información de NH pueden ser graves e impactar directamente en el negocio. Por esta razón, se deben proteger dichos sistemas de información para prevenir, detectar y responder ante este tipo de amenazas.

Medidas de prevención

Los empleados y colaboradores internos y externos de NH deben participar en programas de formación y concienciación para la identificación y métodos de actuación frente a *malware*. Es responsabilidad del Information Security llevar a cabo dichos programas de concienciación.

Se deben implementar soluciones técnicas (antivirus, anti-*malware*) en los equipos, dispositivos y sistemas de información de NH. Para ello, se deben tener en cuenta los siguientes aspectos:

- Los sistemas de información de NH que lo soporten deben tener instalado una solución anti-*malware*, especialmente aquellos que se vean afectados por *software* malicioso (p.e., puestos de usuario final, servidores, etc.).
- Las soluciones anti-*malware* utilizadas deben ser capaz de detectar y eliminar todos los tipos de *malware* conocidos.
- Debe asegurarse que las soluciones anti-*malware* están actualizadas a su última versión y ejecutan análisis periódicos. Las actualizaciones deben instalarse en un entorno de pruebas antes de distribuirse en el entorno de producción.
- La configuración de las soluciones anti-*malware* tiene que estar debidamente protegida. Debe asegurarse que los empleados y colaboradores internos y externos de NH no puedan desactivar ni modificar la solución anti-*malware* sin una autorización previa por parte de Information Security que lo justifique.

- Cualquier sistema de información de NH en el cual no se instale una solución anti-*malware* debe quedar de manera documentada y justificada. Dichas excepciones deben ser autorizadas por Information Security.
- Los sistemas de información de NH que estén dentro del entorno de medios de pago (p.e., números de cuenta, números de tarjetas bancarias, nombres de titulares, códigos de servicio, fechas de vencimientos, etc.) deben ser evaluados de manera periódica para identificar y evaluar posibles amenazas de *malware*.

Medidas de detección

De la misma manera, se deben implementar medidas de detección que permitan identificar código malicioso que pueda afectar a los sistemas de información de NH. Entre estas medidas, destacan:

- Se deben ejecutar escaneos periódicos en todos los sistemas de información de NH. Dichos escaneos serán más estrictos en aquellos sistemas de información críticos para el negocio.
- Las alertas de antivirus deben ser monitorizadas y registradas.
- Cualquier actualización no firmada que deba aplicarse a los sistemas de información de NH debe ser inspeccionada para asegurar que no contiene código malicioso.

Medidas de respuesta

En caso de que se detecte una infección de *malware* en un sistema de información de NH, debe catalogarse como incidente de seguridad. En este caso, Information Security deberá actuar con la mayor celeridad y brevedad posible para asegurar el sistema infectado y evitar la propagación de malware en el resto de sistemas de información, poniendo dichos sistemas infectados en cuarentena.

Los empleados y colaboradores internos y externos deben notificar a Information Security la detección o identificación de *malware* en un sistema de información de NH de la manera más rápida y eficiente posible.

5.7.3. Copias de seguridad

Para hacer posible la recuperación de los sistemas de información de NH y la información contenida en ellos, se deben realizar copias de seguridad de los sistemas de información que traten información titularidad o bajo la responsabilidad de NH. Para ello, se deben establecer las directrices necesarias para la realización, protección, verificación y recuperación de las copias de seguridad.

Realización de copias de seguridad

Para la realización de copias de seguridad, se deben tener en cuenta las siguientes consideraciones:

- El responsable del sistema de información debe definir la amplitud y la frecuencia de la copia de seguridad, basándose para ello en la clasificación de la información almacenada en el mismo. De la misma manera, debe definir el tiempo de retención requerido de acuerdo con los requisitos legales y contractuales a los que esté sujeto.
- Se deben definir guías para la descripción de cómo se deben realizar las copias de seguridad en función de los sistemas de información de los cuales se realiza la copia.

- La ejecución de las copias de seguridad debe ser monitorizada con el objetivo de detectar posibles fallos durante la ejecución de las mismas.
- Siempre que sea posible, la realización de copias de seguridad debe realizarse fuera del horario laboral con la finalidad de no interrumpir el servicio.

Protección de copias de seguridad

Las copias de seguridad deben estar debidamente protegidas. Para ello, se deben implementar las siguientes medidas:

- Las copias de seguridad deben almacenarse en una localización distinta a la localización de los sistemas de información asociados. La distancia entre ambas ubicaciones debe ser suficiente con el fin de prevenir que un desastre que pueda afectar a la localización principal afecte también a la localización donde se almacenan las copias de seguridad.
- El acceso a las copias de seguridad debe estar controlado, permitiendo únicamente el acceso a personal autorizado a las mismas.
- Debe mantenerse un inventario de las copias de seguridad con el fin de identificar las mismas.
- Aquella información que se almacene de forma cifrada, debe permanecer cifrada en las copias de seguridad.

Verificación de copias de seguridad

Se deben llevar a cabo periódicamente pruebas de recuperación de las copias de seguridad, de manera que se verifique:

- La efectividad de los mecanismos para la realización y la protección de las copias de seguridad.
- Nivel de actualización de los procedimientos utilizados para la gestión de copias de seguridad.
- Funcionamiento correcto de los sistemas de información de NH una vez se realice la recuperación de los mismos.

De manera particular, se deben efectuar pruebas de restauración de las copias de seguridad semestralmente en aquellos sistemas de información de NH que traten datos de carácter personal. Dichas pruebas deberán ser documentadas identificando la fecha de la prueba, persona responsable de su realización, información recuperada, ruta del archivo recuperado, fichero al que pertenece la información y el resultado de la prueba.

Recuperación de copias de seguridad

Para llevar a cabo el proceso de recuperación de copias de seguridad, deben establecerse guías que incluyan los pasos a seguir para recuperar la información requerida en los tiempos necesarios. Para la recuperación de dicha información, se debe documentar:

- Persona que solicita la recuperación.
- Responsable de aprobar la recuperación.
- Sobre qué información y sistemas de información de NH se solicita la recuperación.
- Responsable de ejecutar las tareas de recuperación.
- Justificación por la que se solicita la recuperación de la información.

5.7.4. Registros y supervisión

Los sistemas de información o servicios de TI que traten información titularidad o bajo la responsabilidad de NH clasificada como Restringida o Confidencial deben generar registros para permitir el seguimiento de los mismos y garantizar su correcto funcionamiento. De manera general, se establecen las siguientes categorías de eventos:

- Eventos generales:
  - Gestión de usuarios: accesos autorizados y no autorizados por parte de los usuarios, cambios de contraseña, perfiles y privilegios de usuario, inicios de sesión, uso de cuentas de administración, accesos en horarios atípicos.
  - Gestión de sistemas: cambios en políticas, uso de programas de administración, parada y arranque de los sistemas, errores de funcionamiento.
  - Gestión de red: accesos a redes de comunicaciones (autorizados y no autorizados), cambios de políticas.
  - Gestión de incidencias: alertas por prevención de intrusos, mantenimiento del ciclo de vida de las incidencias (incidencias abiertas, creadas, solucionadas), vulnerabilidades de sistema operativo.
  - Antivirus: instancias de antivirus deshabilitadas, registro de sistemas de información infectados.
- Eventos específicos:
  - Firewalls: intentos de ejecución de reglas no permitidas, modificación de la política, tráfico permitido en sistemas que almacenen información confidencial, accesos y desconexiones del usuario administrador del firewall.
  - VPNs: accesos autorizados e intentos de acceso no autorizados, cambios en la configuración del acceso VPN, bloqueo de usuarios.
  - Acceso a Internet: intentos de conexiones no permitidas, accesos realizados fuera del horario laboral, descargas de ficheros con tamaño superior a 10MB.
  - Correo electrónico: buzón de usuario al 90% de la capacidad, identificación de virus conocidos, origen y destino de correos con contenidos adjuntos sospechosos o que superen el tamaño máximo de los mensajes.

Registros (*logs*)

Los sistemas de información de NH deben generar unos registros mínimos. Dichos registros deben contener, de manera general, la siguiente información:

- Dirección IP o nombre del sistema de información que ha generado el evento.
- Identificador del usuario o del proceso.
- Fecha y hora.
- Tipo de evento.
- Descripción o motivo del evento registrado.

En caso de corresponderse con un evento de acceso, se debe registrar:

- Recurso al que se accede.
- Tipo de acceso (lectura, escritura, borrado).
- Si el acceso ha sido autorizado o denegado.

De manera particular, aquellos registros que afecten al entorno de datos de tarjetas de pago deberán registrar:

- Acciones realizadas por los usuarios administradores.
- Accesos a los registros (*logs*) de los sistemas.
- Intentos de acceso lógicos no válidos.
- Cambios de permisos de usuarios y contraseñas.
- Acceso a los datos de tarjetas.
- Creación o eliminación de objetos del entorno.
- Accesos remotos.
- Cambios en los registros (*logs*) de los sistemas.

Almacenamiento y retención de los registros

El almacenamiento de los registros (*logs*) es necesario para que existan futuras investigaciones en caso de ser requerido, siempre respetando las conformidades legales que puedan existir en torno a la privacidad y conservación de la información.

Para ello, debe definirse el periodo de retención de dichos registros. De manera general, el periodo de retención de los registros dependerá de la información contenida en los mismos y del nivel de criticidad de éstos, adecuándose a las conformidades legales a los que estén sujetas.

De manera particular, aquellos registros asociados al entorno de datos de tarjetas de pago, deben conservarse con un mínimo de un (1) año, siendo los tres (3) primeros meses de disponibilidad inmediata para su análisis.

Protección de los registros

Los registros (*logs*) deben ser protegidos y distribuidos de la manera más segura y adecuada posible. Se deben tener en cuenta los siguientes aspectos:

- Los registros deben estar protegidos contra accesos no autorizados.
- Los derechos de acceso a los registros deben concederse según el principio de necesidad de conocimiento.
- Los sistemas involucrados en el procesamiento de registros deben estar situados físicamente en áreas seguras y adaptadas para ello.
- Las transferencias de registros deben estar protegidas con mecanismos que permitan asegurar la integridad de los mismos.
- Las transferencias de registros en redes públicas deben ir cifradas.

Sincronización del reloj

Todos los sistemas de información y servicios de TI del Grupo NH que dispongan de registro de eventos deben tener la fecha y hora exacta y sincronizada para que los registros de eventos sean correctos y consistentes entre sí.

Para ello, deben usarse fuentes fiables de tiempo externas para la sincronización de los servidores de tiempo que sirvan a su vez para la sincronización de los sistemas internos.

Con la finalidad de evitar modificaciones no autorizadas de la configuración de los relojes de los sistemas de información, únicamente el personal autorizado debe tener acceso a la configuración de los sistemas de sincronismo de relojes.

En ningún caso, los empleados o colaboradores internos y externos deben modificar los relojes de los sistemas de información propiedad de NH.

Asimismo, se debe comprobar periódicamente que los sistemas de información tienen un mismo horario uniforme y correcto. Se debe tener en cuenta especialmente los cambios en estaciones horarias y los cambios originados tras las actualizaciones de software o cambios en la configuración.

5.7.5. Gestión de la vulnerabilidad técnica

NH debe establecer un proceso para identificar las vulnerabilidades de seguridad en los sistemas de TI propiedad de NH. Todas las vulnerabilidades deben ser clasificadas según la criticidad y nivel de afectación en dichos sistemas.

Escaneo de vulnerabilidades y test de intrusión

Se deben realizar periódicamente escaneos y análisis de vulnerabilidades en los sistemas de información y en servicios de TI de NH, especialmente en aquellos que son críticos para el Grupo NH. Dichos análisis deben ser autorizados por la Dirección de NH y deben ser realizados por personal cualificado. La periodicidad de los escaneos dependerá de la criticidad de los sistemas de información a analizar.

Como norma general, no se deben realizar escaneos de vulnerabilidades en los sistemas de información de NH durante el horario laboral de trabajo, ya que podría provocar la pérdida de disponibilidad de los mismos.

En particular, aquellos sistemas de información dentro del alcance PCI-DSS, deben ejecutarse escaneos periódicos de manera trimestral mediante herramientas específicas y aprobadas para ello (ASV). Asimismo, los test de intrusión en estos sistemas deben ejecutarse con una periodicidad anual o después de la implementación de un cambio significativo en la infraestructura.

Mitigación de las vulnerabilidades

Los escaneos de vulnerabilidades y test de intrusión deben generar informes en los que se recopile información asociada a cada vulnerabilidad encontrada, con el objetivo de identificar y mitigar dicha vulnerabilidad. Entre esta información se debe recopilar:

- Sistema de información afectado.
- Descripción de la vulnerabilidad.
- Impacto de la vulnerabilidad.
- Servicio afectado.
- Nivel de criticidad de la vulnerabilidad.

- Recomendación.

Es responsabilidad de Information Security velar por la corrección de dichas vulnerabilidades en función del nivel de criticidad.

Gestión de parches

Information Security debe estar suscrito a boletines informativos de seguridad con el fin de estar al corriente de los últimos parches de seguridad publicados por los fabricantes de *software* y *hardware* de la plataforma tecnológica de NH. Dichos parches deben ser analizados e instalados en los diferentes sistemas de información de NH con el objetivo de mantener actualizados los mismos.

Los cambios aplicados para la corrección de las vulnerabilidades identificadas deben ser aprobados y verificados tras su implementación, garantizando la correcta solución adoptada para la corrección de las vulnerabilidades.

Gestión de excepciones

Puede darse el caso de que no sea posible corregir una vulnerabilidad identificada, ya sea porque no existe una contramedida conocida o bien porque la contramedida afecte a la disponibilidad del sistema de información. En este caso, se deben implementar medidas de seguridad que mitiguen el riesgo a la explotación de dicha vulnerabilidad como, por ejemplo:

- Incrementar la monitorización del sistema de información identificado.
- Deshabilitar características del servicio que no sean necesarias y estén relacionadas con la vulnerabilidad identificada.
- Instalación de las utilidades que ayuden a mitigar el riesgo de explotación de la vulnerabilidad.

Dichas excepciones deben ser inventariadas, revisadas y aprobadas por Information Security.

5.8. SEGURIDAD DE LAS COMUNICACIONES

5.8.1. Gestión de la seguridad de redes

Segmentación

El Grupo NH ha definido, como principio general para el diseño seguro de sus redes internas de comunicaciones, el criterio de segmentación, según el cual:

- Se definen diferentes tipologías de redes desde un punto de vista de seguridad, en función de variables como la funcionalidad que ofrecen los sistemas ubicados en la misma, los usuarios de dichos sistemas y el tipo de información intercambiada, el nivel de exposición, etc.
- El nivel de visibilidad entre las diferentes redes se limita al estrictamente necesario.
- Las conexiones entre redes de diferente naturaleza se realizan a través de dispositivos de filtrado adecuados y están sometidas a monitorización mediante Intrusion Detection System (IDS).

En base a los criterios anteriores, NH ha definido las siguientes tipologías de red:

- Redes DMZ: que ofrece servicios accesibles desde redes públicas. Los servicios ubicados en este tipo de redes son aquellos que deben ser visibles desde Internet, o bien, deben estar conectados de forma directa a Internet, tales como portales web, proxys de navegación web, pasarelas de correo, acceso remoto para empleados y colaboradores, etc.
- Redes de producción: en el que se ubican, de manera aislada, los servidores que albergan la lógica de negocio de las aplicaciones y sus activos de información, infraestructura común como servidores LDAP, así como las redes de interconexión con terceros.
- Redes de desarrollo y calidad: en el que se ubican los sistemas que integran los diferentes entornos no productivos utilizados en el Ciclo de Vida de Desarrollo Software.
- Redes de hoteles y oficinas: que permite el acceso a los sistemas de información de NH a los empleados y colaboradores internos y externos a través de sus equipos y dispositivos.
- Redes de gestión: orientado a los sistemas que permiten la monitorización y administración remota de los elementos de comunicación y servidores que soportan la infraestructura tecnológica de NH.

Los requisitos generales de seguridad definidos por NH para las tipologías de red anteriores son los siguientes:

- Los dispositivos de comunicaciones (p.e., switches, puntos de acceso Wi-Fi, etc.) y los dispositivos y sistemas de seguridad (firewalls, IDS/IPS, etc.) son configurados de forma previa a su instalación.
- La realización de cambios en las redes internas de NH a nivel de diseño y/o configuración (p.e., instalación de nuevos servidores, instalación de dispositivos de comunicaciones, modificación de reglas de filtrado, etc.) debe ser notificada con suficiente antelación a Information Security, para la gestión de los riesgos de seguridad de la información.
- Se han definido mecanismos para impedir la divulgación de direcciones IP privadas, información sobre enrutamiento de las redes internas e información sobre los dispositivos a Internet.
- Los componentes de todas las redes de NH, a excepción de los ubicados en la parte pública de las redes DMZ, utilizan direccionamiento privado y direcciones locales únicas.

Redes DMZ

Los servicios ubicados en redes DMZ se dividen en los siguientes grupos según su tipología:

- Servicios públicos: servicios ofrecidos por NH para su acceso a través de redes de acceso públicas.
- Acceso remoto: acceso en remoto a los sistemas de información del Grupo NH ubicados en redes internas por parte de trabajadores y/o proveedores.

NH considera estas redes como de alto riesgo, dado su elevado nivel de exposición frente a posibles atacantes. Por ello, el Grupo NH ha aplicado el principio de defensa en profundidad en el diseño de la arquitectura de seguridad de dichas redes y ha definido un sistema de filtrado basado en doble capa de firewalls.

En el caso de acceso remoto a los sistemas de información de NH por parte de empleados y colaboradores internos y externos se han establecido las siguientes medidas de seguridad:

- Conexión a través de túneles VPN. Política de autenticación de doble factor (usuario y contraseña junto con un token generado por software o un dispositivo hardware).

- El nivel de privilegios de los usuarios (subredes a las que se tiene acceso, navegación a Internet, etc.) se gestiona a través de grupos. Dichos privilegios se limitan a los mínimos necesarios, de acuerdo al criterio de mínimo privilegio.
- Prohibición de utilizar "split tunneling" en el equipo cliente, de modo que se apliquen en dichos equipos únicamente los requerimientos de seguridad a nivel de red fijados.
- Desconexión automática tras un periodo de inactividad de 60 minutos del usuario

Redes de producción

En las redes de producción se debe diferenciar entre las siguientes tipologías:

- Redes de sistemas de información: en las que se ubican los servidores que albergan la lógica de negocio de las aplicaciones, sus activos de información y la infraestructura común (servidores LDAP, etc.)
- Redes de medios de pago: en las que se ubican los sistemas de información de NH que dan soporte a la operativa dentro del alcance de PCI-DSS.

Redes de sistemas de información

Dentro de las redes de sistemas de información, se definen a su vez diferentes redes en función del nivel de sensibilidad de los sistemas que se ubican en ellas.

Dichas redes están siempre aisladas del resto de redes de NH por un elemento de filtrado, a dos niveles:

- La conectividad entre las diferentes tipologías de redes se restringe por defecto. Únicamente se permiten las conexiones estrictamente necesarias en aquellos casos en los que una aplicación deba comunicarse con un sistema ubicado en otra tipología de red diferente.
- En cada una de las tipologías de red, se restringe la conectividad dentro de la misma mediante la definición de subredes. La visibilidad entre las subredes definidas se limita a la estrictamente necesaria para el correcto funcionamiento de las sistemas y servicios.

Redes de medios de pago

Las redes de medios de pago son aquellas en las que se ubican los dispositivos desde los que se procesan transacciones de medios de pago así como los servidores por los que viajan la información asociada a dichos medios de pago (p.e., números de cuenta, números de tarjetas bancarias, nombres de titulares, códigos de servicio, fechas de vencimientos, etc.) Dichas redes se encuentran sometidas al cumplimiento de la normativa PCI-DSS. Para limitar el esfuerzo asociado al cumplimiento de dicha normativa, se tratará de mantener un elevado nivel de asilamiento de este tipo de dispositivos y servidores respecto al resto de redes de NH.

El diagrama de las redes de medios de pago debe permitir la identificación y ubicación de los elementos y sistemas.

Periódicamente, Information Security debe evaluar el nivel de aislamiento aplicado sobre estas redes, así como las medidas de seguridad aplicadas a las conexiones mantenidas desde/hacia estas redes desde el resto de redes internas del Grupo NH.

Redes de desarrollo y calidad

Las redes de desarrollo contienen los sistemas ubicados en los entornos no productivos. Las consideraciones de seguridad son las siguientes:

- Por defecto, la conectividad a dicho entorno se encuentra restringida y el acceso tiene que ser autorizado previamente.
- La conexión entre los entornos de producción y desarrollo está expresamente prohibida.
- Las únicas conexiones permitidas entre entornos de dichas redes, son las necesarias para generar juegos de pruebas, y aquellas conexiones que se establecen para la promoción de software.

Redes de hoteles y oficinas

En estas redes se encuentran los dispositivos de usuario utilizados de forma directa por los empleados y colaboradores internos y externos de NH, así como los servidores ofimáticos. Las redes de usuarios implementan el primer punto de control en el acceso a los activos de información de NH y, por ello, el acceso a dichas redes debe implementar las siguientes medidas de seguridad:

- Los puertos de acceso a la red que estén situados en ubicaciones públicas accesibles por personas ajenas a NH deben restringirse. Por defecto, el acceso a la red a través de estos puertos debe estar restringido y sólo habilitarse cuando sea estrictamente necesario. En todo caso, el control de acceso de usuarios a la red se realiza a través de protocolos que transmitan las credenciales de usuario de forma cifrada a través de la misma.
- Se deben definir diferentes subredes para restringir la visibilidad de los sistemas ubicados en estas redes (p.e., usuarios de ofimática, servidores de ofimática, invitados, PCs administrados por colaboradores externos).

El grado de exposición de las redes inalámbricas (Wi-Fi) las convierte en uno de los eslabones más débiles de la seguridad en redes. Por este motivo, se deben tener en cuenta los siguientes requerimientos:

- Queda prohibida la instalación de redes inalámbricas sin que exista una autorización previa por parte de Information Security. Information Security podrá realizar revisiones orientadas a identificar y detectar puntos de acceso Wi-Fi no autorizados.
- Se deben emplear sistemas de protección seguros (WPA2) y no se pueden crear redes inalámbricas sin protección o que empleen mecanismos de protección considerados inseguros (p.e., WEP, WPA).
- La red para invitados se encuentra totalmente segregada de la red interna de NH y únicamente da acceso al servicio de acceso a Internet, independiente del usado por los empleados de NH.
- Queda prohibido el uso de la red de invitados por los empleados y colaboradores de NH a través de equipos que tengan conexión con las redes internas de NH.
- Las cuentas proporcionadas para acceder a la red de invitados deben tener un periodo de caducidad definido.
- En caso de emplearse portales cautivos para la autenticación de los usuarios, se debe garantizar que las contraseñas empleadas en dichos portales cumplen con la política de contraseñas de NH.
- Se debe evitar el uso de certificados auto-firmados en los portales cautivos para la autenticación de los usuarios en redes de invitados.

Redes de gestión

El tráfico con destino/origen a una red de gestión debe viajar aislado del tráfico de datos a través de redes dedicadas y exclusivas para dicho tráfico de administración.

Debido a la sensibilidad de las acciones realizadas en las redes de gestión, especialmente en cuanto a la administración, se han definido las medidas de seguridad adicionales que se indican a continuación:

- La conexión de un usuario a una red de gestión debe ser autorizada previamente por Information Security y realizarse a través de un sistema de salto, que deberá estar sometido a un nivel de monitorización especial.
- Se deben definir subredes para la administración de sistemas y plataformas especialmente sensibles (p.e, redes de medios de pago).
- La visibilidad entre las diferentes subredes que integran las redes de gestión se encuentra restringida.
- Las credenciales de autenticación de los usuarios se transmiten cifradas dentro de estas redes y en las conexiones que se establezcan con elementos de otras redes internas de NH.

5.8.2. Intercambio de información

Autorización

De manera general, queda prohibido el intercambio de información titularidad o bajo la responsabilidad de NH con terceros ajenos al Grupo NH.

Cuando los empleados y colaboradores internos y externos de NH identifiquen la necesidad de realizar un intercambio de información de NH con un tercero ajeno al Grupo NH, deberán solicitar la autorización al propietario de la información. El propietario de la información tiene la responsabilidad de valorar la necesidad y, en caso de que sea necesario dicho intercambio, ha de poner en conocimiento dicha necesidad a Information Security.

Information Security mantendrá un registro de los intercambios de información clasificada como Confidencial identificados, con el objetivo de que sean incluidos de manera periódica en sus análisis de riesgos.

De manera previa el inicio de un intercambio de información de NH con terceros ajenos al Grupo NH, el propietario de la información debe garantizar que el intercambio se ha regulado en un acuerdo contractual o legal con los terceros, donde como mínimo se desarrollen los siguientes aspectos:

- Las condiciones en las que dichos intercambios tienen lugar.
- Los mecanismos definidos para facilitar la gestión de estos intercambios.
- Las responsabilidades y obligaciones legales de las partes cuando se lleven a cabo los intercambios, especialmente de aquellos afectados por requerimientos normativos.
- Las responsabilidades de control y notificación del envío, transmisión y recepción de la información.
- La necesidad de devolución y/o destrucción de la información intercambiada una vez finalizada la relación contractual.
- Las responsabilidades en el caso de que se produzcan incidentes de seguridad.

El propietario de la información debe estar en contacto con Legal Affairs, con el objetivo de velar por el cumplimiento de normas internas de NH y leyes y reglamentos vigentes.

Intercambio a través de redes públicas

El intercambio de información a través de redes públicas se debe realizar teniendo en cuenta las siguientes directrices generales:

- De manera general, se debe utilizar los mecanismos de intercambio seguro de información proporcionados por NH y autorizados por Information Security (p.e., servidores SFTP, herramientas colaborativas de NH, gestores documentales de NH, etc.)
- Se evitará el intercambio de información clasificada como Restringida o Confidencial a través de canales que no garanticen la seguridad de los intercambios (p.e., correo electrónico sin cifrar, servicios públicos de intercambio de información, SMS, etc.) En aquellos casos en los que el intercambio se produzca a través de canales inseguros, se deben utilizar herramientas de seguridad que garanticen la confidencialidad e integridad del intercambio y que cumplan con los controles criptográficos definidos en la Política de Seguridad de NH, así como en los estándares normativos que emanan de la misma.
- En aquellas situaciones en las que un empleado o colaborador de NH necesite utilizar sistemas de intercambio gestionados por un tercero a través de redes públicas, Information Security es el responsable de realizar un análisis de riesgos de estos sistemas de intercambio y, en función del resultado, autorizar o denegar su uso.

Sistemas de intercambio

Los sistemas de información a través de los cuales se producen los intercambios de información ofrecen la posibilidad de restringir la visibilidad de la información compartida únicamente a los usuarios autorizados, ofreciendo diferentes niveles de granularidad (p.e., entre empleados internos, entre empleados de varios Departamentos, entre empleados internos y colaboradores externos de varios Departamentos, etc.)

Es responsabilidad de los usuarios la definición y administración de los permisos de acceso a la información por parte de otros usuarios.

Medidas de seguridad

Los sistemas de información a través de los cuales se realicen intercambios de información deben atender a las consideraciones de seguridad recogidas en la Política de Seguridad de NH, así como en los estándares normativos que emanan de la misma; en especial:

- Deberán implementar mecanismos criptográficos de protección de la información.
- Deberán ser configurados de acuerdo a las guías de configuración segura autorizadas por NH.
- Deberán generar eventos de seguridad suficientes que permitan el análisis proactivo y la investigación forense de posibles incidentes de seguridad.
- Deberán ser incorporados en el proceso de gestión de vulnerabilidades.

De manera general, los sistemas de intercambio de información serán considerados como repositorios temporales de información. De este modo, se deberá tener en cuenta que:

- No deberán ser empleados como servicios de almacenamiento de información. Por el nivel de exposición de este tipo de servicios, se tratará de minimizar el volumen de información disponible en dichos sistemas.
- La información intercambiada a través de estos servicios, en tanto que se trata de información en tránsito copia de otra información original, no se encontrará protegida por las políticas de copias de seguridad de otros sistemas.
- Se establecerán mecanismos de borrado periódico de la información intercambiada a través de dichos sistemas, con el fin de minimizar el riesgo de robo de información.

Intercambio físico

Respecto a los intercambios de información que se producen a través de soportes u otros medios comúnmente utilizados para el almacenamiento de información (medios ópticos, dispositivos de almacenamiento extraíble, etc.), se deben tener en cuenta las siguientes consideraciones:

- Únicamente se realizará a través de proveedores homologados por NH y con los que se mantenga un acuerdo formalizado. Adicionalmente, se mantendrá un registro de entrada y salida de soportes.
- Los paquetes utilizados en el transporte deberán proteger el contenido del envío de cualquier daño físico durante el transporte y frente a accesos no autorizados (p.e., sobres sellados).
- Se establecerán medidas de seguridad adicionales como el cifrado de los soportes incluidos en el envío.

5.9. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

5.9.1. Requisitos de seguridad en sistemas de información

La incorporación de Information Security en el ciclo de vida del desarrollo de cualquier proyecto informático pretende:

- Garantizar que el nivel de seguridad de los activos de información se encuentra en todo momento alineado con las necesidades de negocio y operacionales de NH, mediante la identificación continua de potenciales riesgos y la correcta aplicación de las correspondientes medidas de seguridad.
- Minimizar el coste de proteger los activos de información, tratando de identificar en las fases tempranas de cualquier proyecto informático las medidas de seguridad que se deberán implantar y el papel que desde Information Security se debe desempeñar.

Es responsabilidad del Responsable de Proyecto notificar a Information Security del inicio de cualquier proyecto informático, una vez haya sido aprobado por cualquiera de los canales de aprobación previstos en el Grupo NH.

Para dichos proyectos, Information Security determina el nivel de involucración que deberá adoptar en cada una las etapas del ciclo de vida del proyecto, en función, entre otras, de las siguientes variables:

- Si se trata del desarrollo de un sistema de información totalmente nuevo o si se trata de la evolución de alguno existente.
- Activos de información afectado/s por el desarrollo del nuevo proyecto, desde el punto de vista del:
    - Del nivel de exposición de los mismos.
    - De los requisitos normativos que le sean de aplicación (p.e., PCI-DSS, GDPR, etc.)
    - De la magnitud y complejidad relativa del proyecto.

Information Security notifica al Responsable de Proyecto la necesidad de su participación en el equipo de trabajo del proyecto, así como el grado de involucración en cada una de las fases del proyecto. En cualquier caso, el Responsable de Proyecto, en el inicio del proyecto y en base a su mayor conocimiento del alcance del mismo, podrá requerir una mayor involucración de Information Security durante el desarrollo del proyecto.

Definición de requisitos de seguridad

Para la formalización de los requisitos de seguridad, durante la fase de Definición de Requisitos se deberán realizar las siguientes tareas:

- Identificar, en función de la información tratada, si el proyecto informático a desarrollar está afectado por requisitos normativos relativos a seguridad de la información. Especialmente, si se procesan datos personales se deben identificar los requerimientos necesarios y proporcionales que garanticen la privacidad desde el diseño y por defecto.
- Realizar un análisis para identificar los riesgos que, desde un punto de vista de seguridad de la información, pueden introducir los cambios asociados al desarrollo del proyecto. El análisis de riesgos deberá contemplar no sólo los riesgos puramente técnicos sino también funcionales, vinculados a la propia operativa de negocio y al uso de los activos de información que se realizará por parte de los usuarios.
- Formalizar el listado de requerimientos de seguridad a satisfacer, que se incorporarán como parte de los requisitos no funcionales del proyecto. La definición de requisitos de seguridad no sólo se centrará en el propio desarrollo del proyecto, sino que también tratará de anticipar los requisitos a tener en cuenta durante la posterior explotación y mantenimiento del mismo. En el caso de que alguno de los requisitos de seguridad pudiera plantear conflictos que bloqueen el desarrollo del proyecto, el Responsable de Proyecto requerirá a Information Security la realización de un análisis formalizado de riesgos, en el que se evaluará si el riesgo asociado es o no asumible y, en su caso, determinar la aplicación de medidas de seguridad compensatorias.

Diseño de la solución

Desde el punto de vista de seguridad, en la fase de Diseño, Information Security podrá colaborar en la ejecución de las siguientes tareas:

- Dar soporte y/o validar el diseño de la solución propuesta, desde el punto de vista de cumplimiento de los requerimientos de seguridad definidos.
- En el caso de que el proyecto así lo requiera, colaborar en el diseño o selección de posibles soluciones de seguridad específicas necesarias para dar cumplimiento a los requisitos de seguridad definidos.
- Definir casos de abuso.
- Diseñar el plan de pruebas de seguridad.

Con respecto al plan de pruebas, si bien éste variará en función de la naturaleza del proyecto informático, NH ha establecido como requisito mínimo, para todos los proyectos que afecten a sistemas expuestos en Internet y/o afectados por la norma PCI-DSS, la inclusión de pruebas de seguridad en el plan de prueba.

Las pruebas de seguridad se realizarán aplicando un enfoque de caja blanca y son las siguientes:

- Revisión del código fuente, mediante herramientas de análisis estático de código.
- Realización de escaneos de vulnerabilidades y test de penetración, tanto a nivel de red como de aplicación, previos a la puesta en producción de la nueva solución.

Desarrollo y construcción

Durante la fase de desarrollo, el equipo de desarrollo del proyecto deberá:

- Atender a las buenas prácticas en la construcción de sistemas:
  - Cuando se trate de proyectos de desarrollo software, asegurando que los equipos de desarrollo conocen y aplican guías de programación segura.
  - Cuando se trate de proyectos de sistemas, a través de las guías de configuración segura de sistemas que los propios fabricantes de sistemas proporcionan.

  Es responsabilidad de Information Security facilitar y formar a IT & Systems respecto a las buenas prácticas en el desarrollo de sistemas seguros
- Ejecutar pruebas específicas de seguridad, siguiendo un enfoque de caja blanca.
  Es responsabilidad del Responsable de Proyecto facilitar un entorno necesario para que las pruebas que se realicen simulen en la medida de lo posible la configuración de seguridad del entorno de producción (p.e., puertos utilizados por la aplicación para su funcionamiento, archivos y/o carpetas a excluir del escaneo de antivirus, etc.)
  Es responsabilidad de Information Security el aprobar las herramientas y procedimientos que den soporte a la ejecución de dichas pruebas y revisar la adecuada ejecución de las mismas.

Pruebas

Antes de la puesta en producción, se deben ejecutar pruebas de seguridad en entornos no productivos aplicando una metodología de caja blanca. Dichas pruebas están orientadas a identificar posibles vulnerabilidades de seguridad presentes en los sistemas de información afectados por los cambios realizados durante el desarrollo del proyecto.

No se podrán poner en producción sistemas para los que durante el desarrollo del proyecto se hayan identificado vulnerabilidades graves de seguridad, sin la aprobación expresa de Information Security ni sin un plan de acción propuesto por el equipo de proyecto que permita corregir dichas vulnerabilidades en un plazo acotado de tiempo.

Puesta en producción

Con independencia de su involucración durante el ciclo de vida de desarrollo del proyecto, de manera previa a la puesta en producción de un nuevo sistema o aplicación, Information Security podrá requerir realizar una auditoría del proyecto con la que verificar el cumplimiento de cada una de las consideraciones anteriormente realizadas en la presente norma. Como resultado de dicha auditoría, Information Security podrá proponer la paralización de la puesta en producción del nuevo desarrollo o sistema.

Una vez aprobada la puesta en producción del nuevo desarrollo o sistema, se debe:

- Actualizar la información necesaria para ejecutar los procedimientos de recuperación ante desastres.
- Actualizar la información necesaria para ejecutar los procedimientos de gestión de vulnerabilidades técnicas.

5.9.2. Seguridad en el desarrollo y en los procesos de soporte

Medidas de seguridad en los entornos no productivos

Se deberá mantener un adecuado nivel de control en aquellos elementos e infraestructura tecnológica que soporten el desarrollo de sistemas. Para ello se deberán establecer, entre otras, las siguientes medidas de seguridad:

- Deberá existir una adecuada segregación de entre los entornos no productivos y los productivos para aislar y caracterizar de una forma adecuada las diferentes funciones y actividades durante el desarrollo.
- Los entornos de desarrollo se deberán mantener protegido frente a:
  - Cambios no autorizados en la configuración.
  - Instalación de software no autorizado.
  - Código malicioso.
  - Accesos no autorizados.
- En la medida de lo posible, se controlará el acceso a Internet desde los sistemas de desarrollo.
- Deberá aplicarse una política consistente de actualizaciones y parches en los equipos de entornos no productivos.
- Deberán aplicarse los procedimientos de gestión de copias de respaldo y recuperación, debiendo estar éstos adecuadamente documentados y ser conocidos por los miembros del equipo de desarrollo.
- Deberá utilizarse un sistema de control de código o versiones sobre el código fuente, de forma que se pueden trazar los cambios realizados sobre los sistemas productivos.

Las librerías de software deberán tener identificado y asignado un propietario, quien definirá qué usuarios tendrán acceso a ellas y qué usuarios tendrán autorización para modificarlas. Asimismo, deberán establecer un adecuado control de versiones y gestión de usuarios que permita:

- Identificar todas las librerías pertenecientes a un sistema.
- Controlar los accesos permitidos.
- Documentar los cambios realizados.
- Delimitar los cambios realizados entre dos versiones de código fuente.

Las librerías de código fuente no se publicarán en el entorno de producción, salvo en aquellos casos en los que los entornos no productivos no permitan compilar código fuente. Las librerías cuyo código ejecutable esté en entornos productivos no se deberán modificar directamente, debiendo trabajar sobre una copia de las mismas.

Segregación de entornos

Los entornos no productivos y los productivos deberán estar separados con el objetivo de conseguir una adecuada segregación de los mismos, evitando, de este modo, incidencias en los elementos del entorno de producción y garantizando la estabilidad e integridad de los sistemas.

Para ello se tendrán en cuenta, en la medida de lo posible, los siguientes requisitos:

- Segregación de entornos:
  - Se deberán diferenciar y separar los entornos no productivos y productivos a través de la dedicación de infraestructuras distintas, ubicadas en segmentos de seguridad diferentes.
  - La única comunicación permitida entre los entornos no productivos y productivos deberá ser la relativa al traspaso de datos, sistemas y servicios de los entornos no productivos a los productivos.
  - Será necesario establecer mecanismos que permitan mantener una trazabilidad de cualquier actividad llevada a cabo en el proceso de desarrollo.
  - No se permitirá, en los entornos de producción, la instalación de herramientas propias de desarrollo de sistemas, como pueden ser: compiladores, editores de código, etc.
  - En ningún caso se llevarán a cabo las actividades asociadas a las pruebas de sistemas en el entorno de producción.
  - Los sistemas de información no productivos deberán, en la medida de lo posible, mostrar mensajes de identificación asociados al entorno no productivo al que pertenecen, con el fin de reducir el riesgo de errores humanos no intencionados durante la actividad del personal sobre los mismos.
- Segregación de funciones:
  - Con carácter general, los perfiles de usuarios con funciones de desarrollo no podrán alterar ni modificar de forma alguna el código albergado en el entorno de producción.
  - Los desarrolladores no podrán acceder al entorno de producción para analizar anomalías y/o posibles incidencias, depurar funcionamiento de aplicativos y servicios, ni para la realización de cualquier actividad relacionada con la función propia de desarrollo. Únicamente podrán acceder al entorno de producción empleando un perfil de usuario final de la aplicación.
  - En los casos excepcionales que, por fuerza mayor, sea imprescindible el acceso del personal con funciones de desarrollo a los entornos de producción, éste deberá estar limitado por una serie de medidas de control. Entre otras, el bloqueo permanente del usuario y desbloqueo durante un tiempo reducido de acceso y, además, deberá ser revisado de forma periódica y regular.

Si en algún caso no se pudiera garantizar la segregación de entornos y/o funciones, se definirán mecanismos y controles de seguridad que mitiguen adecuadamente los riesgos derivados de esta situación. Entre dichos controles, se implantarán los siguientes:

- Revisión de pasos a producción.
- Alertas a través de herramientas de monitorización.
- Inhabilitación de usuarios desarrolladores y habilitación de ventanas de cambios.

Pasos a producción

El entorno de producción es aquel en el que se desarrolla la actividad del Grupo NH. Por este motivo es crítico protegerlo adecuadamente, no sólo frente a accesos o ataques, sino también frente a un proceso de gestión del

cambio inadecuado. Es por ello que se considera necesario definir una serie de medidas que permitan controlar y acotar los cambios que se realicen sobre los sistemas en producción. Para ello se definen las siguientes medidas de seguridad:

- Los cambios en producción deberán estar debidamente identificados y controlados.
- Deberá existir un registro (log) de todos los cambios producidos sobre los sistemas en producción. Para ello, en la medida de lo posible, se recomienda realizar los pasos a producción mediante herramientas destinadas a tal efecto.

Todo paso a producción deberá ser solicitado y, en caso positivo, aprobado, en base al resultado de las pruebas realizadas, es decir, si cumple los requisitos funcionales y de seguridad especificados al inicio del mismo.

- Deberá existir un control de versiones sobre la versión del sistema instalada en producción.
- Las actualizaciones de aplicaciones en los sistemas en producción deberán ser previamente ejecutadas en un entorno de prueba.

5.9.3. Datos de prueba

Con el fin de lograr una adecuada segregación de los entornos no productivos y productivos, se deberán establecer restricciones sobre la copia y acceso a los datos reales del entorno de producción.

Para ello se deberán tener en cuenta los siguientes aspectos:

- En la medida de lo posible se evitará el traspaso o copia de datos reales desde un entorno de producción a un entorno no productivo. Las pruebas llevadas a cabo en los entornos no productivos deberán realizarse con juegos de datos creados a tal efecto.
- En caso de que, por razones del desarrollo, sea imperativo realizar pruebas sobre datos de producción, se tendrán en cuenta las siguientes medidas de seguridad:
    - El proceso de traspaso o copia de datos siempre deberá ser llevado a cabo siguiendo un procedimiento formal, incluso en el caso de que se realice con carácter urgente.
    - En la medida de lo posible, se aplicarán mecanismos de disociación o enmascaramiento que eviten su identificación.
    - En caso de utilizarse datos reales en un entorno no productivo, se deberán pseudoanonimizar o anonimizar de manera previa a la transferencia de dichos datos al entorno no productivo.
    - Los datos traspasados o copiados desde el entorno de producción a cualquier otro entorno, deberán ser eliminados de éstos últimos cuando dejen de ser necesarios o dejen de ser aplicables las causas que originaron la excepción.
    - En el caso de tratarse de datos de carácter personal, y con objeto de garantizar el adecuado cumplimiento de leyes y regulaciones en materia de protección de datos de carácter personal, se deberá asegurar que las medidas de seguridad implantadas en el entorno en el que se almacenen, procesen o trasmitan sean las equivalentes a las exigidas para entornos de producción.
    - En ningún caso se podrán tratar datos reales de medios de pago (números de cuenta, números de tarjetas bancarias, nombres de titulares, códigos de servicio, fechas de vencimientos, etc.) en entornos no productivos.

5.10. RELACIÓN CON PROVEEDORES

5.10.1. Seguridad en las relaciones con proveedores

NH, para la correcta provisión de sus servicios, puede externalizar dichos servicios mediante la contratación de un proveedor, manteniendo una relación contractual entre ambas partes. El enfoque aplicado por NH para la gestión de la relación con sus proveedores de servicio se basa en la definición de un marco de control que contempla todo el ciclo de vida de la relación con dichos proveedores.

Contratación

El responsable de la contratación, empleado interno de NH, deberá rellenar un cuestionario inicial de homologación que permita identificar los controles aplicables para la homologación de dicho proveedor. Asimismo, en base a estas respuestas, el riesgo será evaluado por parte de Information Security una vez sea catalogada la externalización. Para la realización de dicho análisis, los responsables de la contratación deberán comunicar a Information Security el inicio de cualquier proceso de contratación de un proveedor de servicios.

Es responsabilidad de Information Security el análisis de los riesgos asociados a la subcontratación de un servicio con un proveedor. Dicho análisis de riesgos contemplará, entre otras, las siguientes variables de análisis:

- Tipo de servicio prestado.
- Activos de información de afectados por la prestación del servicio.
- Modo de trabajo y acceso del proveedor, distinguiendo entre:
    - Servicio prestado en las instalaciones de NH y/o en las instalaciones del proveedor.
    - Acceso a la información mediante equipos que son propiedad y están gestionados por NH vs. equipos propios del proveedor.

A partir de las conclusiones del análisis preliminar de riesgos realizado por Information Security, se podrán determinar, en cada caso, consideraciones adicionales desde el punto de vista de seguridad de la información a tener en cuenta:

- Durante el proceso de selección del proveedor, introduciendo nuevas variables o requisitos que desde un punto de vista de seguridad será necesario evaluar, bien en forma de requisito de solvencia técnica o bien como parte de los criterios de valoración de las ofertas. Por ejemplo, se podrán considerar:
    - La necesidad de aportar diferentes certificaciones de seguridad de la información.
    - Medidas de seguridad que el proveedor dispone para la prestación de sus servicios.
- Durante el proceso de contratación, imponiendo requisitos y procedimientos de seguridad, adicionales a los mínimos establecidos por NH para cualquier contratación, desarrollados posteriormente en esta norma.

La regulación contractual de los requisitos de seguridad será una de las vías principales aplicadas por NH para la gestión de la relación con sus proveedores. Por ello, en la contratación de proveedores se deberán incluir en los contratos que regirán la contratación los requisitos de seguridad que el proveedor deberá garantizar en la prestación del servicio.

NH establece unos requisitos mínimos de seguridad que deben regularse contractualmente en todos los acuerdos con proveedores de servicios. Estos son los siguientes:

- Aceptación y cumplimiento por parte del proveedor de la Política de Seguridad de NH y de las directrices incluidas en el Cuerpo Normativo de Seguridad que le sean de aplicación. En aquellos casos en los que exista conflicto entre las medidas de seguridad establecidas por NH y las propias del proveedor, se establecerán aquéllas que resulten más restrictivas.
- Acuerdo de confidencialidad: todos los contratos que regulen la relación entre un proveedor y NH incluirán una cláusula en la que el proveedor se comprometa a garantizar la confidencialidad de la información de NH que pueda conocer como consecuencia de la prestación del servicio. Esta obligación no sólo estará vigente durante el periodo de la colaboración, sino que se prolongará de forma indefinida tras la finalización de la misma.
  Asimismo, el clausulado de confidencialidad incluirá la prohibición terminante por parte del proveedor de acceso a toda la información que no sea estrictamente necesaria para la prestación del servicio.
- Clausulado asociado a la protección de datos personales: para los proveedores que presten un servicio que conlleve el tratamiento de datos de carácter personal o bien la prestación de éste prevea de un potencial acceso a los mismos, el contrato incluye el compromiso de cumplimiento de la legislación y normativa aplicable por parte del proveedor.
  Asimismo, quedará establecido que el incumplimiento por parte del proveedor puede ser motivo de rescisión del contrato por parte de NH y/o la reclamación de los daños y perjuicios que dicho incumplimiento ocasionen a NH.
- Clausulado asociado a la protección de medios de pago: para los proveedores que presten un servicio que conlleve el tratamiento de datos reales de medios de pago (números de cuenta, números de tarjetas bancarias, nombres de titulares, códigos de servicio, fechas de vencimientos, etc.) o bien la prestación de éste prevea de un potencial acceso a los mismos, el contrato incluye el compromiso de cumplimiento de la PCI-DSS vigente por parte del proveedor.
- Subcontratación: el proveedor del servicio deberá comunicar obligatoriamente a NH aquellos casos en los que vaya a subcontratar total o parcialmente el servicio que le presta a NH, siempre y cuando en el pliego que rija la contratación no se prohíba explícitamente la subcontratación del servicio. Las obligaciones de seguridad recogidas en el contrato serán de igual aplicación para todos los subcontratistas involucrados en la prestación del servicio.
- Notificación de incidentes de seguridad: el proveedor del servicio tendrá la obligación de comunicar, con la mayor brevedad posible, la ocurrencia de cualquier incidente de seguridad que afecte o pueda haber afectado a la información propiedad de NH y que el proveedor trata como consecuencia de la prestación del servicio.
- Seguridad física: los proveedores que trabajen en las instalaciones de NH, deben cumplir obligatoriamente con las medidas de seguridad física que NH establezca. De manera concreta, se comprometerán a garantizar que todo su personal hace uso de las medidas de seguridad dispuestas por NH para identificar al personal externo que hace uso de sus instalaciones.
  Asimismo, el proveedor deberá garantizar que, a la finalización del contrato, las acreditaciones que permiten el acceso de su personal a las instalaciones de NH son devueltas para su cancelación.
- Gestión de usuarios para el acceso a los sistemas de información de NH: los proveedores que requieran de acceso a los sistemas de información de NH deberán cumplir con las siguientes pautas:
  - Facilitar los datos identificativos del personal del equipo de trabajo, para la adecuada gestión de las cuentas de usuarios en los sistemas de información de NH.

- Comunicar cualquier modificación en la composición del equipo de trabajo, para que NH pueda gestionar de manera adecuada el alta y las bajas a sus sistemas de información.

- Revisión de cumplimiento: el contrato de prestación de servicios establecerá expresamente la obligación del proveedor en cuanto al cumplimiento de la Política de Seguridad de NH y de las normativas legales aplicables, pudiendo NH supervisar dicho cumplimiento en el momento y forma en que se estime oportuna.
- Devolución de la información: contractualmente quedará reflejado la obligación por parte del proveedor de destruir y/o devolver la totalidad de la información de NH a la que haya podido tener acceso como consecuencia de la prestación del servicio.

La regulación contractual de los requisitos de seguridad anteriores aplica a la totalidad de contratos y constituyen los mínimos exigibles por NH.

Por ello, y sin perjuicio de lo anterior, Information Security podrá establecer requisitos complementarios en función del análisis de riesgo anteriormente descrito.

Administración y seguimiento

La gestión diaria de la relación con los proveedores será realizada, fundamentalmente, por el responsable de la contratación que externalice el servicio.

De esta forma, para garantizar que la prestación del servicio cumple con los requisitos de seguridad de la información establecidos por el NH, el responsable de la contratación que externalice los servicios subcontratados deberá llevar a cabo las siguientes tareas:

- Velar porque los proveedores conozcan y cumplan la Política de Seguridad de NH y las medidas de seguridad que le sean de aplicación.
- Notificar las altas, bajas y modificaciones de las cuentas de usuario utilizadas por el personal del proveedor y definir los privilegios de acceso, con el fin de garantizar que los privilegios de acceso a los sistemas de información se mantienen actualizados y se basan en el principio de mínimo privilegio.

Asimismo, es responsabilidad de Information Security velar por el cumplimiento de los requisitos de seguridad establecidos en la contratación del servicio. Esta función de seguimiento se basará en la revisión periódica del cumplimiento de los requisitos de seguridad establecidos en la contratación del servicio, que se podrá articular de manera diferente para para cada uno de ellos: la solicitud de vigencia de certificaciones, informes de auditoría de terceras partes, revisiones ad-hoc, etc.

La ejecución de cualquier cambio en la provisión del servicio deberá ser aprobada por el responsable de la contratación. De esta manera, el impacto en la seguridad de cualquier cambio que se realice y afecte al servicio prestado, debe ser evaluado conjuntamente entre Information Security y el proveedor de servicios antes de llevarse a cabo dicho cambio.

Es responsabilidad de Information Security conservar un registro actualizado de los proveedores de servicios TI, incluyendo su categorización del riesgo y el resultado del análisis de riesgos realizado.

Finalización

La última etapa definida en la gestión de la relación con un proveedor de servicios es la finalización de la relación entre éste y NH. Con el fin de gestionar adecuadamente los riesgos asociados a la finalización de la relación, se definen los siguientes requerimientos:

- Se deben revocar todos los privilegios de acceso concedidos al personal del proveedor, contemplando:
  - Acceso físico: A través de la devolución y cancelación de tarjetas de acceso, códigos de acceso, llaves, etc.
  - Acceso lógico: Mediante la revocación de las cuentas de usuario utilizadas por el proveedor para el acceso a los diferentes sistemas de información, incluyendo los permisos para acceso remoto a los sistemas de NH.
- Se debe garantizar la destrucción y/o la devolución de los activos de información por parte del proveedor a NH, así como de los activos físicos (equipos portátiles, tokens para acceso remoto, teléfonos, etc.) propiedad de NH.

El responsable de la contratación debe notificar a Information Security la fecha de finalización de los contratos y, conjuntamente, garantizar el cumplimiento de los requerimientos anteriores.

5.11. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

5.11.1. Gestión de incidentes de seguridad de la información y mejoras

Procedimientos y responsabilidades

NH debe definir los procedimientos y responsabilidades necesarios para la correcta gestión de los incidentes de seguridad de la información. Para ello, se definen:

- Empleados y colaboradores internos y externos de NH: deben notificar cualquier tipo de incidencia de seguridad o indicio de la misma a Information Security en la mayor brevedad posible.
- Equipo de resolución: son los encargados de ejecutar las acciones necesarias para contener y resolver los incidentes. Deben reportar periódicamente el estado de los incidentes tratados y recolectar las evidencias necesarias para posteriores investigaciones periciales.
- Legal Affairs & Compliance: deben valorar si es necesario emprender acciones legales.
- Information Security:
  - Analizar las incidencias reportadas y descartar falsos positivos.
  - Supervisar la fase de contención y resolución de incidentes.
  - Escalar y reportar los incidentes a terceras partes.
  - Notificar a las partes interesadas todos aquellos incidentes que supongan un incidente grave de seguridad de la información, como aquellos que afecten a datos de carácter personal o al entorno de datos de tarjetas de pago.

El proceso de gestión de incidentes de seguridad de la información de NH contempla todas las fases del ciclo de vida de un incidente de seguridad, desde su detección hasta el cierre.

Detección

Tipos de incidencias

La tipología de incidencias de seguridad es de naturaleza variable, se contemplan, aunque no exclusivamente, los siguientes casos: denegación de servicio; fuga de información; ataque lógico interno; ataque lógico externo; malware; actividad ilegal o ilícita; pérdida de equipamiento; violaciones de las políticas internas del Grupo NH; etc.

Identificación de incidencias

La identificación de incidentes de seguridad de la información se puede producir por medio de dos vías:

- Externa a Information Security: a través de los empleados, colaboradores internos o externos, clientes, las Fuerzas y Cuerpos de Seguridad del Estado, o terceras organizaciones con las que NH pueda mantener algún tipo de relación.
  Con independencia del origen de la incidencia, es obligación de todos los empleados y colaboradores internos y externos notificar a Information Security cualquier incidencia de seguridad que detecten en la mayor brevedad posible. Es responsabilidad de Information Security:
  - Definir y difundir los canales formales de notificación de incidentes de seguridad.
  - Formar y concienciar a los empleados y colaboradores internos y externos de NH respecto a cómo identificar y reportar una incidencia de seguridad.
- Interna a Information Security: a partir de la vigilancia proactiva de amenazas que se pueda realizar mediante la explotación de herramientas de monitorización de seguridad. Es responsabilidad de Information Security definir los requisitos en cuanto a generación de registros (*logs*) de seguridad que se deberán generar en los sistemas de información de NH y de las herramientas necesarias para explotar de manera proactiva dichos registros.

Evaluación de incidencias

Una vez notificada la incidencia, el equipo responsable de la misma debe realizar un análisis preliminar de la incidencia. Para llevar a cabo este análisis debe recabar cuanta información acerca de la incidencia sea necesaria. Al menos la siguiente información debe recolectarse:

- Fecha y hora exacta en la que se detectó la incidencia.
- Persona que ha detectado la incidencia.
- Personas, sistemas, ubicaciones o información que han sido comprometidos.
- Registros (*logs*) y otras evidencias necesarias para evaluar la naturaleza de la incidencia.
- Responsables de la resolución de la incidencia.

A partir de esta información, Information Security realiza las siguientes acciones:

- Valorar si se trata realmente de una incidencia o si se trata de un falso positivo.
- Evaluar el impacto potencial de la incidencia, clasificarlo como incidente y proceder a su registro.
- Comunicar a todas aquellas partes afectadas aquellos incidentes que supongan un incidente grave de seguridad de la información. Asimismo, deben establecerse los mecanismos necesarios para

comunicar a las autoridades correspondientes aquellas incidencias que afecten al entorno de datos de tarjetas de pago o a información de carácter personal, entre otros.

Registro de incidencias

Todos los incidentes de seguridad de la información identificados deben quedar registrados en un único repositorio de información, que permita:

- Mantener un registro histórico de las incidencias de seguridad gestionadas por el Grupo NH.
- Generar un mínimo nivel de información de las acciones realizadas por NH durante la gestión de cada uno de los incidentes.

Resolución

Contención del incidente

La primera etapa de la gestión de un incidente debe ser la contención del mismo, con el objetivo de minimizar el potencial impacto que pueda generar el incidente. El objetivo de esta etapa no es el de identificar la causa raíz del problema sino el de minimizar su impacto y evitar que el incidente se propague y pueda afectar a nuevos activos que en un principio no se habían visto afectados.

Recolección de evidencias

Con el fin de habilitar la posibilidad de emprender acciones legales, tanto penales como civiles, contra una persona u organización que haya originado un incidente de seguridad o; en el caso de que como consecuencia del incidente se hayan visto comprometidos datos de medios de pago o datos de carácter personal, durante todo el proceso de gestión del incidente se deberá asegurar la recopilación de las evidencias que pongan de manifiesto la ocurrencia del incidente. Este proceso de recopilación debe garantizar la validez de las mismas, mediante:

- El establecimiento de controles que permitan garantizar la calidad e integridad de las evidencias.
- El cumplimiento de normativas o códigos de buenas prácticas para la elaboración de pruebas.

A continuación, se establecen las pautas a seguir para garantizar la calidad e integridad de las evidencias recopiladas y que por lo tanto puedan ser admitidas como prueba en un proceso judicial:

- En caso de tratarse de documentos en papel: se debe guardar una copia del documento original de forma segura con un registro de la persona que encontró el documento, dónde y cuándo lo encontró y quién presenció el descubrimiento. Se debe garantizar que el documento original no ha sido alterado.
- Si se tratase de información en soportes informáticos: se deben realizar imágenes o copias exactas de cualquier medio extraíble y de la información en discos duros o en la memoria para garantizar su disponibilidad.
- Es necesario mantener un registro de todas las acciones que se han llevado a cabo durante el proceso de copia y dicho proceso debe ser presenciado por otra persona. Los soportes originales y el registro se deben almacenar en un lugar seguro para evitar accesos no autorizados a los mismos.

Resolución del incidente

La contención del incidente no siempre implica haber resuelto la causa por la cual se materializó el incidente. Una vez contenido el incidente, el equipo de resolución debe dar los siguientes pasos:

- Identificar la causa raíz del incidente.
- Proceder con la resolución de la causa raíz introduciendo las contramedidas que se consideren oportunas y posteriormente verificando su efectividad.

El equipo de resolución debe mantener informado a Information Security de manera periódica y documentar todas las acciones realizadas durante la gestión del incidente. Los miembros del equipo de resolución no podrán facilitar información relacionada con la gestión del incidente a terceros ajenos al propio equipo de resolución o a Information Security.

Asimismo, si el equipo de resolución asignado es incapaz de resolver la incidencia, debe escalar dicha incidencia a otros equipos de resolución más experimentados según los procedimientos y canales establecidos.

Durante todo el proceso de gestión del incidente, Information Security debe monitorizar el grado de avance conseguido y asume la responsabilidad única de reportar frente a terceros cualquier información relacionada con el incidente.

Cierre

Reporte

A la finalización de cualquier incidente de seguridad, el equipo de resolución del incidente deberá generar un informe formalizado del caso, que contenga, al menos, la siguiente información:

- Origen del incidente.
- Impacto ocasionado.
- Acciones realizadas durante la gestión del caso, tanto durante la contención como en la resolución del mismo.
- Propuesta de acciones previstas para minimizar la probabilidad de ocurrencia de nuevos incidentes similares.

Acciones legales

A partir de las conclusiones obtenidas del informe de cierre del incidente, Information Security junto con el Legal Affairs, y si aplica Compliance, evaluarán la necesidad de poner los resultados de las investigaciones realizadas a disposición de People o de los Comités internos de NH facultados para emprender las correspondientes acciones legales que se pudieran derivar de dicho incidente.

Mejora continua

Con el fin de contribuir a la mejora continua del proceso de gestión de incidentes de seguridad, periódicamente o bajo petición, Information Security elaborará informes ejecutivos relacionados con dicho proceso.

El contenido de dichos informes deberé contemplar aspectos tales como:

- Volumen y naturaleza de incidencias de seguridad gestionados en el proceso.

- Análisis de causas raíz de incidencias recurrentes y propuesta de planes de acción para corregirlas.
- Seguimiento de los planes de acción propuestos como consecuencia de los incidentes de seguridad gestionados en el periodo.

5.12. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

5.12.1. Continuidad de la seguridad de la información

La continuidad de la seguridad de la información es tenida en cuenta por NH en el proceso de gestión de la continuidad de negocio.

Planificación

En relación a la planificación de la continuidad de la seguridad de la información, Information Security es la responsable de:

- Definir los requerimientos de seguridad de la información que se deben tener en cuenta en la planificación del proceso de gestión de la continuidad de negocio.
- Supervisar que los requerimientos de seguridad de la información incluidos en la fase de planificación son implantados en los sistemas de información de respaldo.
- Analizar nuevos aspectos relacionados con la seguridad de la información en el proceso de gestión de la continuidad de negocio, con el objetivo de identificar nuevos requerimientos de seguridad de la información aplicables en situaciones adversas.

Implementación

NH debe establecer, documentar e implementar procesos, procedimientos y controles que aseguren el nivel requerido de seguridad de la información durante una situación adversa.

Information Security debe asegurar que existe:

- Personal con autoridad y competencia para responder ante incidentes de seguridad.
- Procedimientos de recuperación en los que se detallen requerimientos de seguridad específicos.

De acuerdo con los requerimientos de continuidad de la seguridad de la información, se deben establecer, documentar, implementar y mantener:

- Controles de seguridad de la información dentro de los procesos, procedimientos, sistema soporte y herramientas utilizadas para la gestión de la continuidad negocio.
- Controles compensatorios que sirvan para mitigar los controles de la seguridad de la información que no puedan mantenerse durante una situación adversa.

Revisión y actualización

NH debe verificar periódicamente o después de un cambio significativo, que los controles de seguridad en el marco de la continuidad de negocio se encuentran implementados de forma correcta, con el objetivo de asegurar que estos controles son efectivos en situaciones adversas.

Dichas verificaciones de controles son llevadas a cabo durante las pruebas del plan de continuidad de negocio para aprovechar las sinergias existentes.

5.12.2. Contingencia tecnológica

El Grupo NH ha diseñado e implementado una arquitectura de contingencia tecnológica que permite cumplir con los requerimientos de disponibilidad definidos por el negocio.

Asimismo, se dispone de los siguientes procedimientos formalizados y documentados:

- Procedimientos organizativos, utilizados para declarar una situación de contingencia, gestionar dicha situación y, una vez finalizada, volver a la normalidad.
- Procedimientos técnicos, utilizados a modo de guía detallada para recuperar un sistema concreto y/o una determinada arquitectura tecnológica. Dichos procedimientos son muy exhaustivos con el fin de permitir independizar la persona responsable de su ejecución.

El correcto funcionamiento de la arquitectura de contingencia tecnológica y sus procedimientos asociados es probado de manera periódica. Este proceso se encuentra documentado y formalizado y es llevado a cabo por los proveedores responsables de la gestión de la infraestructura de tecnologías de la información y supervisado por Information Security.

5.13. CUMPLIMIENTO

Para cumplir con los requerimientos legales y contractuales deben tenerse en cuenta los siguientes aspectos:

- Identificar la legislación existente relacionada con la seguridad de la información.
- Adaptar los sistemas de información, procesos y responsabilidades de acuerdo con la legislación identificada.
- Respetar los derechos de propiedad intelectual.
- Proporcionar la protección apropiada a los registros de información que son relevantes o esenciales desde el punto de vista legal.
- Asegurar el cumplimiento de las leyes de protección de datos personales.

5.13.1. Cumplimiento de los requisitos legales y contractuales

Identificación de la legislación aplicable y de los requisitos contractuales

La identificación de nuevos requerimientos legales y contractuales relacionados con la seguridad de la información, se lleva a cabo en NH a través de Legal Affairs, Compliance e Information Security.

Debe considerarse cualquier legislación que envuelva alguno de los siguientes aspectos:

- Protección de información privada y datos personales.
- Derechos de propiedad intelectual.
- Acciones legales debido a negligencias o incumplimientos de contrato.
- Recolección de evidencias en caso de incidentes de seguridad.
- Exportación de datos a otros países.
- Requerimientos de seguridad en los sistemas o en las comunicaciones.
- Monitorización de la información y derechos del usuario.
- Protección de registros.
- Requisitos de seguridad en contratos con proveedores.
- Prevención de blanqueo de capitales.
- Legislación específica para transacciones económicas realizadas electrónicamente.

La identificación de nuevos requisitos normativos permite a NH:

- Definir planes de adecuación a los nuevos requisitos normativos identificados, ya sea en forma de proyecto liderado por Legal Affairs & Compliance o Information Security, o enmarcando su ejecución dentro de iniciativas de otras áreas.
- Actualizar la Política de Seguridad de NH y los estándares normativos que emanan de la misma. En este sentido, se debe tener en cuenta que, en su contenido, la Política de Seguridad de NH trata en todo momento de dar cumplimiento a los marcos regulatorios que son de aplicación sobre los sistemas de información.
- Definir los requerimientos de seguridad a tener en cuenta durante el desarrollo de nuevos proyectos.
- Definir los requerimientos de seguridad a tener en cuenta en las relaciones con los proveedores.
- Actualizar el catálogo de riesgos, amenazas y vulnerabilidades, de manera que sea tenido en cuenta de cara a la planificación y ejecución de los ejercicios de análisis de riesgos.

Por último, las áreas y departamentos involucrados en el proceso son responsables de la interlocución directa con auditores externos, organismos reguladores, fuerzas y cuerpos de seguridad del estado, y terceros en general; en lo relacionado con la acreditación del nivel de cumplimiento por parte de NH de las respectivas regulaciones que le sean de aplicación.

Derechos de la propiedad intelectual

Todas las actividades relacionadas con información o material sujeto a los derechos de propiedad intelectual deben considerar las restricciones legales relacionadas con esta materia.

Deben establecerse acuerdos con los fabricantes y/o propietarios de productos *software* y *hardware* o material protegido (p.e., documentos, informes, etc.) con el fin de cumplir con los derechos de propiedad intelectual. Únicamente se puede utilizar *software* no licenciado cuando haya sido desarrollado por el propio Grupo NH o haya sido cedido por los desarrolladores.

Los empleados y colaboradores internos y externos de NH están informados sobre los derechos de propiedad intelectual y conocen la prohibición de copiar aplicaciones protegidas por derechos de autor, así como la prohibición de uso de aplicaciones para las que no se dispone de licencia.

Protección de los registros de la organización

Los registros de información relevantes o esenciales desde el punto de vista legal (p.e., datos financieros, contables o cualquier dato relevante desde el punto de vista regulatorio) deben protegerse con el fin de evitar fugas, pérdidas o alteraciones indebidas.

A tal fin, se encuentran implantadas medidas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de dichos registros.

Protección y privacidad de la información de carácter personal

La protección de cualquier tipo de información personal que sea procesada de forma automática o manual debe garantizar el honor y la privacidad de los individuos, así como el ejercicio pleno de sus derechos.

Las medidas de seguridad de carácter técnico y organizativo, así como las responsabilidades asignadas para cumplir con la legislación vigente en materia de protección de datos se detallan en el "Documento de Seguridad" de NH y sus anexos.

5.13.2. Revisiones de la seguridad de la información

Cumplimiento de la Política de Seguridad

NH entiende la seguridad de la información como un proceso de mejora continua, y no como un estado. De esta forma, la realización de revisiones periódicas tiene como objetivos:

- Verificar el cumplimiento de la Política de Seguridad de NH, así como de los estándares normativos que emanan de la misma, por parte de los empleados y colaboradores internos y externos del Grupo NH.
- Mejorar la Política de Seguridad de NH y, por consiguiente, el modelo de seguridad de NH. La ejecución de revisiones de cumplimiento contribuye a:
    - o Identificar desviaciones en la eficacia operativa de los controles y/o en su diseño.
    - o Identificar nuevas necesidades en materia de seguridad.
    - o Mantener actualizado los estándares normativos que emanan de la Política de Seguridad de NH.

Revisión independiente de la seguridad de la información

Con periodicidad anual, se debe elaborar un Plan de revisiones de seguridad de la información en el que se detallan las revisiones y análisis de seguridad que deberán llevarse a cabo en el próximo ejercicio. Dicho Plan se incluye en el Plan táctico de Information Security para cada ejercicio. De igual forma, las revisiones, análisis y evaluaciones externas que afecten a IT & Systems serán coordinadas por Information Security.

Para la elaboración del citado Plan, se deben tener en cuenta, entre otros, los siguientes factores:

- El Mapa de Riesgos de Seguridad de la Información de NH.
- Los incidentes de seguridad ocurridos durante el último ejercicio.

- Los requisitos de carácter regulatorio que afecten a los sistemas de información.

La ejecución de cada uno de las tareas de las revisiones que componen el Plan deberán ser planificadas:

- Se identificarán los interlocutores clave tanto de IT & Systems como de los colaboradores incluidos en el alcance de la evaluación.
- Los responsables de IT & Systems, así como de los colaboradores incluidos en el alcance de la revisión, deberán facilitar cuanta información les sea solicitada por Information Security para el desarrollo de la misma.
- Se acordará con los anteriores interlocutores el alcance de la revisión, los plazos de ejecución y el modo de acceso a la información necesaria para ejecutar la auditoría.

La persona designada como responsable de la revisión, evaluación o análisis de seguridad en ningún caso dependerá jerárquicamente del responsable del Área o Departamento auditado, asegurando así la independencia de los resultados.

De igual forma, en el caso de las revisiones de carácter técnico que deban realizarse sobre los sistemas de producción de NH, la ejecución de los trabajos de auditoría deberá atenerse a las siguientes consideraciones:

- Todas las pruebas que puedan afectar a la disponibilidad de los sistemas de NH deben ejecutarse en periodos de baja actividad (p.e., fuera de horario laboral).
- Las pruebas sobre sistemas de producción no pueden modificar o borrar datos. Aquellas pruebas que necesiten modificar o borrar datos para probar la existencia de una vulnerabilidad, deberán ejecutarse siempre en un entorno de pruebas aislado.
- Todas las comprobaciones y pruebas que se realicen sobre los sistemas deberán quedar registradas y evidenciadas.
- Las herramientas que se utilicen para realizar pruebas sobre los sistemas de producción deberán estar licenciadas y soportadas; y deberán haber sido homologadas de manera previa a su utilización.

Los resultados de las revisiones, evaluaciones y análisis de seguridad realizadas y/o coordinadas por Information Security serán reportados al Comité de Seguridad y se planificarán planes de acción asociados para corregir las debilidades identificadas. En aquellas de carácter técnico en las que durante el desarrollo de las mismas se detecten vulnerabilidades muy graves, no será necesario reportar todos los resultados, sino que se podrán reportar resultados de manera aislada para anticipar la aprobación de los planes de acción correspondientes.

Los resultados de las revisiones, evaluaciones y análisis de seguridad realizadas o coordinadas por Information Security servirán de igual base para elaborar el Plan Director de Seguridad del Grupo NH.

6. CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

Las presentes normativas proporcionan cobertura a aspectos recogidos en los siguientes estándares de seguridad reconocidos internacionalmente:

- Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (ISO/IEC 27001)
- Tecnología de la información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. (ISO/IEC 27002)
- Payment Card Industry Data Security Standard (PCI DSS)

Para el desarrollo de la presente política se han tomado como referencia los requerimientos legales previstos en legislaciones de los principales estados donde opera el Grupo NH, tales como el GDPR, la LOPD, la LPI o la LSSI.

7. DOCUMENTOS RELACIONADOS

- ALLNH-POL100-ES - Política de Seguridad
- ALLNH-NOR201-ES - Glosario de términos y definiciones