NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

Madrid, 13 de febrero de 2025

Autor/es: Responsable de Seguridad de la Información y DPO
Validado por: Comité de Gestión Integrado
Aprobado por: Órgano de Administración

Proyecto: Sistema de Gestión Integrado (SGI)
Clasificación: Público

ÍNDICE DE CONTENIDOS

1. INTRODUCCIÓN

NWorld es consciente de la importancia de la seguridad de la información y protección de datos personales como factor clave para alcanzar la excelencia organizativa, la competitividad en el mercado, la sostenibilidad del negocio y el cumplimiento normativo.

El grupo, en consecuencia, con lo anterior, ha establecido en la organización los procesos de planificación e implantación de controles, así como de supervisión y mejora, con el fin de garantizar la confidencialidad, la integridad, la autenticidad, la trazabilidad y la disponibilidad de la información y de los servicios.

El presente documento tiene por objeto implantar la política en materia de seguridad de la información y protección de datos personales, establecer las buenas prácticas para el uso seguro de los activos que dan respuesta al desarrollo de dicha política, y definir las responsabilidades del personal y de los usuarios en referencia a las materias de referencia.

Este documento se integra en el Sistema de Gestión Integrado (SGI) de NWorld. Todo su contenido es de obligado conocimiento y cumplimiento por parte de todo el personal y los empleados de terceras partes que tengan acceso a la información manejada, y en especial a los datos automatizados de carácter personal y a los sistemas de información.

La Documentación de Protección de Datos se encuentra a disposición de quien la desee consultar, previa solicitud al delegado de protección de datos (dpo@nfq.es).

2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES v5.0

La presente Política establece las directrices y líneas de actuación en materia de Seguridad de la Información que rigen el modo en que NWorld gestiona y protege su información y sus servicios, así como la comunicación con sus clientes y otros grupos de interés.

2.1 Misión y marco regulatorio

La seguridad de la información forma parte del ADN de NWorld, siendo ésta su actividad de servicios principal, por lo que debe formar parte de todas las actividades que se desarrollen tanto a nivel interno como, muy especialmente, en aquellas operaciones que formen parte del servicio al cliente, teniendo en cuenta que la información es el activo más crítico de la compañía.

NWorld se asegura de la implementación de la presente política de la seguridad de la información que sirve de bastidor y permite el desarrollo de los objetivos del Sistema de Gestión de la seguridad de la información de acuerdo con la ISO/IEC 27001 y el Esquema Nacional de Seguridad. La implementación de estas normas son un factor estratégico para la continuidad y mejora del negocio, de modo que NWorld requiere seriedad y rigurosidad en los procedimientos con el objetivo de obtener una madurez suficiente en el Sistema de Gestión de la Seguridad de la Información. Además, considera que la seguridad de su información es un valor básico para la continuidad del negocio.

Por otro lado, NWorld trata datos personales que deberán mantenerse inventariados por tratamiento, con el objeto de facilitar el control, la gestión y la protección de los mismos, aplicando medidas para cumplir con el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Por último, el SGSI/ENS de NWorld se mantendrá cumpliendo y respetando la Ley de Propiedad Intelectual en lo que se refiere al uso del software, obteniendo las licencias correspondientes y llevando un registro y control de estas para el empleo adecuado de éstas en el desarrollo de las actividades.

NWorld se asegura de que todas las personas que la integran conozcan y apliquen el SGSI. Para ello, se encuentra a disposición de todos los/las trabajadores/as un documento llamado “Buenas prácticas en SI” y la presente política SSI.

La política de seguridad se establecerá de acuerdo con los principios básicos señalados en el capítulo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y se desarrollará aplicando los requisitos mínimos establecidos en el ARTÍCULO 12. POLÍTICA DE SEGURIDAD Y REQUISITOS MÍNIMOS DE SEGURIDAD.
Así mismo, se ajustará a lo establecido en la ley 59/2003 por el “Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior” y añadir la “Ley 6/2020, de 11 de noviembre,

reguladora de determinados aspectos de los servicios electrónicos de confianza”
Se establecen las siguientes propiedades en el intercambio de información en todas aquellas situaciones y relaciones con clientes y entre los trabajadores, en las que NWorld forma parte activamente, donde se almacena, procesa o transmite la información para su intercambio:

- **Confidencialidad:** NWorld asegura que sólo quienes estén autorizados puedan acceder a la información.
- Integridad: NWorld asegura que la información y sus métodos de proceso sean exactos y completos, evitando modificaciones no autorizadas.
- **Disponibilidad:** NWorld asegura que únicamente los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.
- **Autenticidad:** NWorld asegura que la información provenga de una fuente de origen fidedigna, es decir, que el origen sea realmente quien envía la información.
- **Trazabilidad:** NWorld asegura que las acciones de una entidad se puedan rastrear únicamente hasta dicha entidad.

2.2 Principios fundamentales

Con el propósito de propiciar y mantener las propiedades descritas, NWorld realiza sus actividades y alienta su negocio mediante los siguientes principios fundamentales:

- Compromiso con el cumplimiento de los requisitos del marco legal y regulatorio en el que se desarrollarán sus actividades, así como las indicaciones de seguridad de la información que el INCIBE y el CCN recomiendan.
- Establecer los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
- Priorizar la gobernanza de la gestión del riesgo y la seguridad de la información como elemento fundamental para la continuidad de los servicios, estableciendo la estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización.
- Proteger el activo de la información frente a amenazas de acuerdo con los criterios internos de aceptación del riesgo, conforme a las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
- Aplicar el concepto de mejora continua, involucrando a toda la organización, a sus aliados y a los grupos de interés, para la consecución de los objetivos.

2.3 Objetivos

- Tratar los datos personales con licitud, lealtad y transparencia, persiguiendo la limitación de la finalidad, minimización de datos, exactitud, integridad, confidencialidad, limitación del plazo de conservación, y responsabilidad proactiva.
- Tratar y custodiar la información propia y la de los clientes preservando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad en todos los momentos de su proceso.
- Adaptar sus sistemas a entornos cambiantes, gestionando los nuevos riesgos, Adecuando las capacidades de la infraestructura, y fomentando el trabajo en equipo y su cohesión dentro de la organización.

2.4 Compromiso y liderazgo

Todas las personas que integran NWorld comprenden y son responsables de cumplir estos principios, así como todas las sistemáticas de seguridad de la información

aprobadas que los desarrollan.
El Órgano de Administración de NWorld se compromete a facilitar y proporcionar los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora del SGSI/ENS de la entidad, así como a demostrar liderazgo y compromiso respecto a este, a través de la constitución del Comité de Seguridad de la Información que tendrá la responsabilidad de:

- Asegurar el establecimiento de la presente política y los objetivos de la seguridad de la información, y que estos sean compatibles con la estrategia de NWorld
- Asegurar la integración y el cumplimiento de los requisitos aplicables del SGSI/ENS en los servicios y procesos de la entidad.
- Asegurar que los recursos necesarios para el SGSI/ENS estén disponibles.
- Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del SGSI/ENS.
- Asegurar que el SGSI/ENS consigue los resultados previstos.
- Dirigir y apoyar a las personas para contribuir a la eficacia del SGSI/ENS.
- Promover la mejora continua.
- Apoyar otros roles pertinentes del Órgano de Administración, liderando a sus áreas de responsabilidad en seguridad de la información. El detalle de las funciones específicas del Comité de Seguridad de la Información, se describen en su acta de constitución.

2.5 Funciones y responsabilidades de seguridad de la información

El **Comité de Seguridad de la Información** procederá a revisar y a proponer la aprobación de la presente Política de Protección de Datos Personales y Seguridad de la Información a la Órgano de Administración de NWorld y será el **Responsable de la Información** y de los **Servicios**.
Además, el **Comité de Seguridad de la Información** centralizará los mecanismos de coordinación y resolución de conflictos entre los responsables que se indican a continuación, que se tratarán mediante debate durante las reuniones de los miembros de dicho comité y que serán moderados por la Dirección General:

- El **Comité de Seguridad** de la Información, en representación de la Órgano de Administración de NWorld, será el órgano encargado de aprobar la política y será la responsable de la autorización de sus modificaciones, así como de toda la información documentada del SGSI/ENS de la entidad.
- El **Responsable de Seguridad de la Información** será el encargado de notificar la presente política al personal de la entidad y de los cambios que en ella se produzcan, así como de coordinar las acciones de implantación,

mantenimiento y mejora del SGSI/ENS de la entidad (incluyendo la firma de la Declaración de Aplicabilidad que formaliza la relación de medidas de seguridad aplicables derivadas del Análisis de Riesgos), y de sus auditorías, junto con el **Responsable de IT** que se encargará de gestionar los requisitos técnicos de seguridad de los sistemas de información.

- El **Responsable de cada información y/o del servicio** afectado por el análisis y gestión de riesgos se indicará en el Mapa de Riesgos del SGSI/ENS de NWorld que recogerá los criterios que determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 40 y los criterios generales prescritos en el Anexo I del Real Decreto del ENS.
- El **Delegado de Protección de Datos Personales** será el encargado de garantizar que los datos personales se tratan y se protegen conforme al Reglamento General de Protección de Datos (RGPD UE 2016/679), por lo que trabajará en coordinación con el **Responsable de Seguridad de la Información** y con el **Responsable de IT**.
- Todo el **personal de la organización**, tanto interno como externo, será responsable de cumplir con la presente Política de Protección de Datos Personales y Seguridad de la Información dentro de su área de trabajo, así como de aplicar toda la información documentada de los controles y medidas de seguridad del SGSI/ENS de NWorld en sus actividades laborales que afecta a su desempeño en seguridad de la información.

.

3 GUÍA DE USO ACEPTABLE DE ACTIVOS. v4.0

3.1 El uso seguro de la información es responsabilidad de todos.

Para la implantación efectiva de las buenas prácticas de uso seguro de los activos de información, NWorld proveerá los medios necesarios, factibles y proporcionados, de acuerdo con un modelo de mejora continua, haciendo especial énfasis en la formación del personal y en el control y análisis de los resultados para verificar la eficiencia y eficacia de las prácticas.

El Responsable de Seguridad de la información implantará las medidas de seguridad de la información para dar cumplimiento de las buenas prácticas de uso seguro de los activos de información y, así mismo, supervisará su cumplimiento, por parte de todo el personal y los empleados de terceras partes que tengan acceso a la información manejada por NWorld.

3.2 Uso seguro de equipos, comunicaciones y aplicaciones.

Para garantizar el buen uso de los equipos que se entregan a los usuarios y las aplicaciones instaladas en los mismos, se seguirán las siguientes medidas:

- A todos los usuarios se les asignará un equipo propiedad de NWorld, debidamente inventariado y puesto a su disposición exclusivamente para la realización de las funciones dentro de la empresa.

- Todos los equipos y sistemas son propiedad de NWorld. Éstos son asignados a los usuarios, debidamente inventariados y puestos a su disposición exclusivamente para la realización de las funciones en la empresa.
- La instalación y uso de cualquier software, ajeno a los instalados o autorizados expresamente, queda terminantemente prohibida. Asimismo, las modificaciones a los elementos del hardware entregado deberán ser realizadas exclusivamente por miembros del departamento de IT.
- Todos los programas software instalados en los equipos contarán con las debidas licencias de uso y/o mantenimiento emitidas por sus fabricantes.
- No está permitido el uso de ordenadores, teléfonos móviles, ni cualquier otro soporte o dispositivo propiedad de NWorld para asuntos personales.

3.3 Acceso físico controlado.

Para garantizar el debido acceso físico a las dependencias de NWorld donde se ubican los equipos y sistemas de información, se seguirán las siguientes medidas:

- El acceso físico de personas no pertenecientes a NWorld a las dependencias, estará controlado en la recepción y deberá ser autorizado previamente por el responsable de la unidad a la que se vaya a visitar.
- El acceso de las visitas estará en todo momento monitorizado por NWorld.
- Las visitas que accedan a las zonas donde se albergan los equipos y sistemas de información deberán estar en todo momento acompañadas por personal de NWorld.

3.4 Puesto de trabajo despejado.

Para garantizar la protección de la información con la que se trabaja en el día a día en el puesto de trabajo, se seguirán las siguientes medidas:

- Mientras se esté en el puesto de trabajo se debe conservar sobre el escritorio solamente los documentos necesarios.
- Cuando se abandona el escritorio de forma temporal, se debe guardar la información sensible en un sitio seguro y activar el bloqueo de pantalla.
- Al abandonar el escritorio al final del día se deben archivar cualquier elemento con información sensible y apagar el equipo de trabajo.
- En cuanto a las impresoras, se deben retirar los documentos, asegurándose que no queda nada en la bandeja.

3.5 Medios de protección

Para garantizar la protección de los equipos, instalaciones generales y dependencias de NWorld donde se ubican los equipos y sistemas de información, se seguirán las siguientes medidas:

- La disposición de medios de detección de incendios.
- La disposición de aparatos de medición de temperatura y humedad.

- La protección de las redes y canalizaciones de datos.
- Acceso restringido a CPDs y almacenes.
- Control de acceso a las oficinas.

3.6 Identificación y autentificación de los usuarios.

Para garantizar el debido acceso a los equipos, programas informáticos y datos, se seguirán las siguientes medidas:

- A todo el personal de NWorld se le asigna un nombre de usuario, personal e intransferible, que tendrá asociado privilegios en función de las necesidades de su puesto.
- Las contraseñas serán configuradas por el departamento de IT de NWorld, cumpliendo los requisitos establecidos en la Política de Uso de Controles Criptográficos y Gestión de Claves. Deberán ser cambiadas en el primer inicio de sesión, y deben renovarse de acuerdo a la Política de Uso de Controles Criptográficos y Gestión de Claves (entre 45 y 90 días).
- Los privilegios serán modificados o eliminados en el momento que se produzca un cambio en las funciones de su puesto, o la baja en NWorld, respectivamente.

3.7 Uso seguro de internet.

Para garantizar el acceso a Internet y el uso correcto de sus recursos por parte de los usuarios, se seguirán las siguientes medidas:

- El tráfico a internet desde las oficinas es monitorizado y controlado por NWorld en todo momento.
- NWord implementará mecanismos para evitar el acceso a contenidos inseguros y/o inapropiados desde equipos corporativos.
- Por su parte, el usuario está obligado a respetar las restricciones de acceso a contenidos y zonas inseguras e inapropiadas, de acuerdo con las prácticas de buen uso reconocidas y la legislación vigente.

3.8 Uso seguro del correo electrónico.

Para garantizar el debido uso del correo electrónico por parte de los usuarios, se seguirán las siguientes reglas:

- A todo usuario de NWorld se le asignará una dirección de correo electrónico, personal e intransferible, para el desempeño de sus actividades profesionales dentro de la empresa.
- Las cuentas de correo electrónico asignadas a los usuarios son propiedad de NWorld.
- Los contenidos de los correos electrónicos son confidenciales, de acuerdo al ordenamiento legal.

- A cada cuenta de correo creada se le asignará una contraseña inicial que deberá ser cambiada por el usuario inmediatamente después de haber iniciado sesión.
- Las contraseñas deberán cumplir los requisitos establecidos en la Política de Uso de Controles Criptográficos y Gestión de Claves. Deben renovarse de acuerdo a la Política de Uso de Controles Criptográficos y Gestión de Claves (90 días).
- El usuario deberá configurar el Doble Factor de Autenticación (MFA) con algunos de los mecanismos habilitados.
- Como reglas generales se recomienda:
- No abrir o reenviar mensajes de correo de remitentes desconocidos.
- No abrir o reenviar mensajes de correo de remitentes conocidos, pero con asuntos en idiomas diferentes a su remitente.
- No abrir los ficheros adjuntos de correos de procedencia dudosa.

3.9 Uso seguro de los dispositivos móviles.

Para garantizar el debido uso de los dispositivos móviles (teléfonos inteligentes, tabletas y ordenadores portátiles) por parte de los usuarios, se seguirán las siguientes reglas:

- No utilizar dispositivos propiedad de NWorld para asuntos personales.
- Dentro de lo posible, conectarse sólo a redes de confianza.
- No dejar el dispositivo móvil desatendido en lugares públicos.
- Los ordenadores portátiles desatendidos se suspenderán de acuerdo a lo establecido en la Guía de Puesto de Trabajo Despejado y Equipo Desatendido (en general, tras 3 minutos de inactividad).
- Los intentos de inicio de sesión fallidos de forma reiterada provocarán el bloqueo de la cuenta de usuario durante un tiempo definido. Las condiciones de bloqueo y recuperación quedan establecidas en la Política de Uso de Controles Criptográficos y Gestión de Claves (3 intentos fallidos provocan 3 minutos de bloqueo).
- Se recomienda conectar los dispositivos a la red por cable siempre que sea posible, y desactivar la conectividad WIFI.
- Mantener deshabilitada la conectividad bluetooth siempre que no se esté utilizando.
- El acceso remoto a la red de NWorld se realizará a través de conexiones VPN. Desde el departamento de IT se facilitarán los medios para ello.
- NWorld proporcionará una herramienta para la transferencia de información confidencial a través de internet. El acceso a esta herramienta se debe solicitar al departamento de IT de NWorld.
- Mantener la información relevante almacenada en la herramienta corporativa proporcionada por NWorld (Google Drive).

3.10 Uso seguro de dispositivos de almacenamiento externo.

La utilización de dispositivos de almacenamiento externo queda bloqueada para todos los usuarios de NWorld, con la excepción de miembros del departamento de IT y personal expresamente autorizado y justificado por sus funciones.

3.11 Filtrado de contenidos maliciosos y protección de los sistemas operativos y otras utilidades

Para garantizar la identificación, el bloqueo y eliminación de contenidos potencialmente maliciosos, el departamento de IT de NWorld instala y mantiene un sistema antivirus en todos los equipos de los usuarios.

Para garantizar la eficacia del sistema antivirus y reducir los riesgos y vulnerabilidades derivadas de los sistemas operativos y de otras utilidades instaladas en los equipos de los usuarios es de obligado cumplimiento la observación de las siguientes medidas:

- Reiniciar el ordenador siempre que sea necesario para finalizar la instalación de las actualizaciones del antivirus.
- Tomar acciones correctoras cuando el antivirus lo recomiende.
- Informar al departamento de IT de cualquier comportamiento anómalo del dispositivo.

3.12 Datos personales.

Para evitar incidencias derivadas del manejo de los datos de carácter personal, con el apoyo del Delegado de Protección de Datos (DPO) de NWorld, se seguirán las siguientes medidas:

- Identificar los soportes que contengan datos de carácter personal y su nivel de protección, así como los usuarios que tengan acceso a los mismos.
- Dar seguimiento a los controles para el cumplimiento de la legislación vigente en materia de protección de datos personales.
- Supervisión del correcto tratamiento de la información, por parte del Responsable de Seguridad de la Información y el DPO de NWorld, para cumplir los procedimientos de seguridad definidos.
- Queda prohibido el almacenamiento de datos personales sin previa autorización del responsable de los mismos.
- Se deberán borrar los ficheros temporales que contengan datos personales una vez se haya cumplido con la finalidad para la que fueron creados.
- La configuración de las aplicaciones que tratan datos personales sólo podrá ser modificada con la autorización del responsable de seguridad o por el administrador de sistemas.
- Los soportes que contengan datos personales, y vayan a ser desechados o reutilizados, deberán pasar por un proceso de eliminación segura que imposibilite el posterior acceso a la información que ha estado contenida en los mismos.

- La salida fuera de la organización de soportes informáticos que contengan datos de carácter personal precisa la autorización del responsable de los ficheros.
- Los soportes que contengan datos de carácter personal deberán ser almacenados de manera que quede restringido su acceso al personal no autorizado.
- Evitar transmitir o comunicar datos considerados sensibles por redes públicas.
- La información deberá ser archivada y manipulada con total diligencia para asegurar su disponibilidad, integridad y confidencialidad.
- Queda terminantemente prohibido comunicar a cualquier persona ajena a la organización cualquier información a la que haya tenido acceso en el desempeño de sus funciones

3.13 Copias de seguridad.

Para garantizar la recuperación de los datos almacenados por los usuarios en caso de pérdida o destrucción, se seguirán las siguientes medidas:

- La información almacenada en dispositivos móviles será responsabilidad del usuario. Para prevenir la pérdida de datos, éste deberá mantener la información relevante almacenada en la herramienta corporativa proporcionada por NWorld (Google Drive).
- La información relevante almacenada en servidores y otros dispositivos será respaldada por NWorld de acuerdo a las políticas establecidas.
- Las copias de seguridad serán custodiadas y conservadas por NWorld de acuerdo al Procedimiento de Gestión de Copias de Seguridad.

3.14 Protección de la información.

Para evitar la pérdida, robo o transferencia no autorizada de la información clasificada o propiedad intelectual de NWorld se seguirán las siguientes medidas:

- La identificación y clasificación de toda la información, en cualquier soporte, considerada de especial protección.
- El seguimiento y supervisión de los controles para el acceso, manejo, transmisión y reproducción de dicha información.
- El seguimiento por los usuarios de una práctica de puesto de trabajo despejado de expedientes y bloqueo de pantalla cuando el equipo esté desatendido o no esté en uso.

3.15 Gestión de las incidencias.

Para mitigar y corregir cualquier incidencia relativa a los sistemas de información y comunicaciones y evitar su repetición, se seguirán las medidas siguientes:

- Comunicación inmediata al Responsable de Seguridad de la Información de NWorld de cualquier evento, incidente o anomalía que afecte a la información y que se considere urgente y/o grave por su impacto (algunos ejemplos

pueden ser: comportamiento anómalo de aplicaciones, indisponibilidad de recursos, pérdida de control de los programas, desconexión súbita, comunicación externa sospechosa, presencia física de desconocidos no identificados en las dependencias, etc.) a través del correo seguridad@nfq.es

- Registro y seguimiento de las incidencias reportadas por los usuarios hasta su solución y cierre.
- Análisis periódico de las incidencias para la propuesta de medidas correctivas o preventivas y toma de decisión por el Comité de Seguridad de la Información de NWorld.

3.16 Continuidad de las operaciones.

Para reducir los riesgos derivados de la ocurrencia de un accidente, catástrofe, atentado o sabotaje de los equipos, personal, sistemas e instalaciones de NWorld se seguirán las siguientes medidas:

- La preparación y actualización periódica del plan de continuidad de negocio.
- La difusión y formación sobre las medidas de continuidad de negocio entre el personal y los colaboradores.

3.17 Mejora continua.

Para optimizar y mejorar de modo permanente la gestión de la seguridad de la información, se seguirán las siguientes medidas:

- La presente guía será revisada anualmente o, en el caso de que se produzcan cambios significativos, para asegurar su continua idoneidad, adecuación y eficacia.
- Mantener un registro de las versiones, que identifique las validaciones por el Comité de Gestión Integrado de NWorld.
- La propuesta de cualquier sugerencia, medida o idea, por medio de correo electrónico, por parte de los usuarios al Responsable de Seguridad de la Información de NWorld. El registro y seguimiento hasta su cierre, aceptación o desestimación, de las mejoras propuestas.
- El análisis de las mejoras propuestas y aceptación o desestimación por el Comité de Gestión Integrado de NWorld.
- El reconocimiento público de los que propongan mejoras.

3.18 Activos propiedad de los clientes.

En aquellos casos en los que los clientes entregan al personal de NWorld dispositivos de su propiedad para la prestación de los servicios, el uso de los mismos seguirá las mismas reglas y medidas que para los dispositivos propiedad de NWorld, salvo que el cliente disponga otras medidas. Además:

- El cliente podrá monitorizar y revisar las comunicaciones, el trabajo realizado y la información contenida en los mismos, con la finalidad de evitar un uso inapropiado de los activos, de acuerdo al ordenamiento legal.

- No está permitida la realización de cualquier actividad que suponga recabar o extraer datos de los dispositivos entregadis, hacia dispositivos que no sean propiedad del cliente
- El empleado debe comunicar a su responsable directo de NWorld, con la mayor brevedad posible, cualquier daño o malfuncionamiento en el material facilitado por el Cliente.

3.19 Condiciones de uso de la red corporativa.

Los usuarios de la red corporativa deben hacer un uso responsable de la misma bajo el principio de buena fe, respetando la legalidad vigente y los derechos de terceros y evitando perjudicar, sobrecargar o deteriorar el servicio o causar cualquier daño a la infraestructura.

En concreto, a título meramente enunciativo y con carácter no exhaustivo, no se podrá usar la red corporativa para:

- Realizar actividades ilegales.
- El uso de redes de intercambio de archivos P2P (Bit Torrent, eMule, etc.), descargas directas de páginas no oficiales (Mega, Rapid, etc.) y el acceso a URLs con contenido spam o cualquier otro acceso peligroso a webs de dudosa confianza.
- Actuaciones que puedan producir daños y/o alteraciones no autorizadas en servicios y/o equipos.
- Remitir mensajes utilizando una identidad falsa y/o camuflar en manera alguna el origen del mensaje.

4 RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN DEL PERSONAL Y DE LOS USUARIOS.

4.1 Responsabilidades generales del personal de NWorld.

- Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal.
- Divulgar y hacer cumplir a las personas de su dependencia la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal.
- Utilizar los controles y medios que se hayan establecido para los activos de información (datos, soportes, equipos) asignados a los usuarios de su área de responsabilidad.
- Utilizar los controles y medios que se hayan establecido para proteger los datos de carácter personal que se traten en su área de responsabilidad.
- Impedir accesos indebidos al código fuente de los desarrollos propios o para terceros.

- No intentar saltar los mecanismos y dispositivos de seguridad, evitar cualquier intento de acceso no autorizado a datos o recursos e informar de posibles debilidades en los controles
- Guardar secreto sobre los datos que pueda conocer, así como sobre controles y posibles debilidades, incluso después de haber causado baja en la organización
- Usar de forma adecuada los mecanismos de identificación y autenticación ante los sistemas de información, tanto sean contraseñas como sistemas biométricos u otros, mediante acceso local o a través de redes de comunicaciones.
- No ceder ni comunicar a otros las contraseñas, personales e intransferibles, que no estarán almacenadas en claro, y que serán transmitidas por canales seguros.
- Evitar transmitir o comunicar datos considerados sensibles por redes públicas
- Cumplir la normativa de gestión de soportes informáticos que contengan datos de carácter personal, así como tomar precauciones en el caso de soportes que vayan a desecharse o ser reutilizados, mediante la destrucción, inutilización o custodia.
- No sacar equipos o soportes de las instalaciones sin la autorización necesaria, y en todo caso con los controles que se hayan establecido
- En caso de finalizar su relación laboral, devolver todos los activos en su posesión.

Todas las obligaciones y compromisos anteriores deben mantenerse, incluso después de extinguida la relación laboral. Asimismo, se recuerda que el usuario será responsable frente al responsable de los datos y frente a terceros de cualquier daño que pudiera derivarse para unos u otros del incumplimiento de los compromisos anteriores.

El incumplimiento de la política y los procedimientos de seguridad de la información de NWorld puede derivar en acciones tales como la retirada, temporal o definitiva, de los derechos de acceso a la información, incluyendo la apertura de un proceso disciplinario o cese de la relación laboral, en aquellos en los que las consecuencias sean graves o muy graves, debidas a actuaciones deliberadas o malintencionadas.

Durante el proceso disciplinario se deberán asegurar tres parámetros de proporcionalidad:

- Asegurarse de que esa persona ha cometido efectivamente la infracción.
- Evitar tratamientos injustos o incorrectos.
- Producir una respuesta gradual, tomando en cuenta la gravedad, el impacto, si es deliberada o si existe repetición.

A tal efecto, a continuación, se procede a establecer, de conformidad con el Convenio Colectivo, y con las normas vigentes del ordenamiento jurídico laboral, las sanciones que la empresa podrá aplicar, según la gravedad y circunstancias de las faltas cometidas, atendiendo a su importancia, reincidencia e intención, a saber:

- Faltas leves: son aquellas motivadas por la no observancia de la Guía de uso aceptable de los activos, sin que sus consecuencias provoquen incidencias

que afecten a la continuidad del negocio o a la confidencialidad o integridad de los datos, ni causen incumplimiento legal alguno.

Las faltas leves podrán ser sancionadas como sigue:

a. Amonestación verbal.
b. Amonestación por escrito.
c. Suspensión de empleo y sueldo un día.

- Faltas graves: aquellas motivadas por la inobservancia deliberada de la Guía de uso aceptable de los activos, que hayan provocado o hayan podido provocar incidencias que afecten a la continuidad del negocio, la confidencialidad o integridad de la información o hayan causado algún incumplimiento legal.

  Las faltas graves podrán ser sancionadas como sigue:

a. Suspensión de empleo y sueldo de uno a diez días.
b. Inhabilitación, por plazo no superior a un año, para el ascenso a la categoría superior.

- Faltas muy graves: aquellas motivadas por la inobservancia deliberada de la Guía de uso aceptable de los activos, que hayan provocado o hayan podido provocar incidencias que afecten a la continuidad del negocio con impacto relevante en el servicio a los clientes, una brecha en datos de carácter personal o de información sensible, el daño en la reputación o imagen pública de la empresa o un incumplimiento legal con expediente sancionador.

  Las faltas muy graves podrán ser sancionadas como sigue:

a. Pérdida temporal o definitiva de la categoría profesional.
b. Suspensión de empleo y sueldo de once días a dos meses.
c. Inhabilitación durante dos años o definitivamente para ascender a otra categoría superior.
d. Despido.

La empresa comunicará a los empleados el anterior régimen sancionador.

Para la aplicación de las sanciones que anteceden se tendrán en cuenta el mayor o menor grado de responsabilidad del que cometa la falta, categoría profesional del mismo y repercusión del hecho en las demás personas trabajadoras y en la empresa.

5 MEJORA CONTINUA.

Para optimizar y mejorar de modo permanente, se seguirán las siguientes medidas:

- El presente documento será revisado anualmente, o cuando corresponda en el caso de que se produzcan cambios significativos, para asegurar su continua idoneidad, adecuación y eficacia.
- La propuesta de cualquier sugerencia, medida o idea, por medio de correo electrónico, por parte de los usuarios al Responsable de Seguridad de la Información (seguridad@nfq.es) o DPO (dpo@nfq.es). El registro y seguimiento hasta su cierre, aceptación o desestimación, de las mejoras propuestas.

- El análisis de las mejoras propuestas y aceptación o desestimación por el Comité de Gestión Integrado de NWorld.
- El reconocimiento público de los que propongan mejoras.