NORMATIVA DE USO DE LOS SISTEMAS

INFORMACIÓN DE USO INTERNO

DE ACCESO INTERNO AL PERSONAL DE NICE PEOPLE AT WORK

Cuadro de Control

Título:	Normativa de uso de los sistemas
Tipo de documento:	Normativa
Nombre del fichero:	NO-Normativa de uso de los sistemas
Clasificación:	Uso interno
Estado:	Aprobado
Autor:	Recursos Humanos y Responsable de Seguridad

Revisión y aprobación		
Revisado por:	Responsable de Seguridad	22/07/2024
Revisado por:	Head of Legal	22/07/2024
Aprobado por:	Comité de Seguridad	22/07/2024
Aprobado por:	Consejo de Administración	

INDICE

1. OBJETO

El objeto del presente documento es establecer la normativa de uso de los sistemas de información en NPAW (en adelante, la Organización).

La seguridad siempre ha sido un concepto presente en todos los sistemas de gestión de la información. Su implementación no es sencilla, dado que abarca todos los eslabones de la cadena de gestión de la información y requiere de un gran conjunto de medidas organizativas y tecnológicas.

El éxito de su implantación depende además de que exista en todos los niveles una cultura de la seguridad, es decir, una concienciación sobre la necesidad de que la información se mantenga en secreto, íntegra y disponible.

Uno de los eslabones normalmente más débiles de la cadena de gestión de la información es precisamente el Usuario final del sistema (informático y papel), debido en gran parte al desconocimiento de la importancia que tiene la seguridad de la información.

El Usuario final necesita, por tanto, ser concienciado y culturizado en materia de seguridad de la información y al mismo tiempo debe disponer de unas normas de obligado cumplimiento respecto al uso de los sistemas informáticos a su alcance, así como soportes o documentos en papel. Y, con especial relevancia, en cuanto a preservar la confidencialidad de la información de carácter personal que esté siendo tratada en cumplimiento de la legislación vigente.

El presente documento establece, así, las normas de uso de los dispositivos asignados al puesto de trabajo, la red corporativa, equipos portátiles, aplicaciones informáticas, así como sobre el acceso y tratamiento de datos de carácter personal, a nivel informático y en papel.

Es fundamental que todos los empleados de la Organización que utilizan equipamiento informático y accedan o traten información de carácter personal para la realización de sus funciones y tareas sean conocedores de esta norma.

2. ALCANCE

Esta normativa es de aplicación a todo el ámbito de actuación de la Organización, y sus contenidos traen causa de las directrices de carácter más general definidas en el ordenamiento jurídico vigente, en la Política de Seguridad de la Información y en las Normas de Seguridad de la Organización

La presente normativa es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la Organización, especialmente, el Responsable de Seguridad, los responsables de Sistemas de Información y los propios usuarios, como actores ambos, en sus respectivas competencias, de la especificación de la normativa de control de acceso, de la implantación técnica de dicha normativa, y del

cumplimiento de la misma, incluyendo, en su caso, el personal de proveedores externos, cuando proceda y sean usuarios de los Sistemas de Información de la Organización.

3. NORMATIVA Y JURISPRUDENCIA

En las entidades es cada vez mayor la utilización de las nuevas tecnologías, lo que ha creado, en ciertas circunstancias, la necesidad de control de estas herramientas por parte del empresario. No obstante, ello puede suponer una quiebra de la intimidad del trabajador constitutiva de un delito contra la intimidad.

Aun así, este derecho a la intimidad del trabajador debe conciliarse con los derechos e intereses legítimos del empleador, como el derecho a velar por la eficacia de la entidad y protegerse del perjuicio que pudiera ocasionar a la entidad las acciones del trabajador.

Es interesante hacer una breve referencia a la normativa y jurisprudencia existente en esta materia:

El Convenio Europeo para la Protección de los Derechos Humanos establece que toda persona tiene derecho al respeto de la vida privada y familiar, y prohíbe la injerencia que no esté prevista en la ley y que no se justifique por razones de seguridad, bienestar económico, defensa del orden, prevención de las infracciones penales, protección de la salud, de la moral o de los derechos y libertades de los demás.

Asimismo, nuestra Constitución Española, recoge como derecho fundamental el derecho a la intimidad personal y familiar y a la propia imagen, así como el secreto de las comunicaciones.

Por su parte, el Estatuto de los Trabajadores, en su art. 20, dispone que el empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.

Los Tribunales han interpretado esta cuestión y, como ejemplo, la sentencia del Tribunal Supremo, de 26 de septiembre de 2007 (Sala de lo Social), establece lo siguiente:

"…las medidas de control sobre los medios informáticos puestos a disposición de los trabajadores se encuentran, en principio, dentro del ámbito normal de esos poderes: el ordenador es un instrumento de producción del que es titular el empresario "*como propietario o por otro título*" y éste tiene, por tanto, facultades de control de la utilización, que incluyen lógicamente su examen.

Por otra parte, con el ordenador se ejecuta la prestación de trabajo y, en consecuencia, el empresario puede verificar en él su correcto cumplimiento, lo que no sucede en los supuestos del artículo 18, pues incluso respecto a la taquilla, que es un bien mueble del empresario, hay una cesión de uso a favor del trabajador que delimita una utilización por éste que, aunque vinculada causalmente al contrato de trabajo, queda al margen de su ejecución y de los poderes empresariales del artículo 20 del Estatuto de los Trabajadores para entrar dentro de la esfera personal del trabajador.

[…] Se trata de medios que son propiedad de la empresa y que ésta facilita al trabajador para utilizarlos en el cumplimiento de la prestación laboral, por lo que esa utilización queda dentro del ámbito del poder de vigilancia del empresario, que, como precisa el artículo 20.3 del Estatuto de los Trabajadores, implica que éste "*podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales*", aunque ese control debe respetar "*la consideración debida*" a la "*dignidad*" del trabajador".

Asimismo, la mencionada sentencia estableció que existe un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la empresa a los trabajadores. Esta tolerancia crea una expectativa de confidencialidad que debe ser tenida en cuenta.

Por ello, dispone a continuación que **las empresas deben fijar previamente las reglas de uso de los instrumentos de trabajo** (p.ej: estableciendo prohibiciones absolutas o parciales, o permitiendo el uso personal por parte de los empleados) **y deben informar a los trabajadores** -y a sus representantes legales, de haberlos- de cuáles son esas reglas, de los controles y medidas aplicables por parte de la empresa. De este modo desaparece la expectativa de intimidad de los trabajadores sobre esos medios y su control no debería generar un posible delito contra la intimidad.

Aunque esta doctrina se ha flexibilizado en virtud de sentencias posteriores del Tribunal Supremo y del Tribunal Constitucional, es recomendable que las empresas dispongan de un protocolo de actuación en materia de uso de TIC's.

4. ROLES Y RESPONSABILIDADES

Responsable de Seguridad	● Elaborar la normativa de uso de los sistemas de información.
Comité de Seguridad	● Aprobar la normativa de uso de los sistemas de información.
Usuarios	● Cumplir con la normativa de uso de los sistemas de información.

5. CUERPO DEL DOCUMENTO

5.1. Propiedad y uso de los dispositivos

La Organización facilita a los Usuarios el equipamiento informático necesario para la realización de las tareas relacionadas con su puesto de trabajo.

Propiedad de los recursos. Este equipamiento es propiedad de la Organización y, por tanto, no está destinado a un uso personal. Como consecuencia de esto, la Organización se reserva el derecho de revisar, sin previo aviso, los equipos y el uso de Internet y el teléfono corporativo que esté haciendo cada Usuario, en caso de que existieran indicios de que se está llevando a cabo una utilización indebida. De esta forma, el usuario queda informado de que el resultado de los controles efectuados puede ser utilizado para llevar a cabo, en su caso, las actuaciones disciplinarias previstas por la normativa vigente.

Obligaciones de los usuarios. Los Usuarios deben cumplir las siguientes medidas de seguridad para el uso de los ordenadores personales:

Conexión de otros dispositivos	● No está permitido conectar dispositivos que no estén autorizados a la red de la Organización. ● Tampoco se pueden conectar a los dispositivos autorizados, otros dispositivos que no estén autorizados expresamente.
Uso de dispositivos y de la red	● Los dispositivos, así como la red de información que la Organización pone a disposición de los usuarios, están destinados a permitir el desempeño de las funciones y tareas profesionales que estos tienen encomendadas, estando prohibido el uso para la realización de actos desleales o que pudieran ser considerados ilícitos.
Antivirus	● El Usuario deberá comprobar que su antivirus se actualiza con regularidad. En caso contrario, deberá notificarlo como una incidencia de seguridad.
Uso de la información	● Está prohibido utilizar, copiar o transmitir información contenida en los sistemas informáticos para uso privado o cualquier otra distinta del servicio al que está destinada. ● El Usuario se abstendrá de copiar la información contenida en los ficheros en los que se almacenen datos de carácter personal u otro tipo de información, responsabilidad de NPAW en ordenador

	o teléfono móvil propio, pendrives o a cualquier otro soporte informático, salvo que solicite autorización al Responsable de Seguridad, y se adopten las medidas de seguridad correspondiente. Asimismo, los datos contenidos en este tipo de soportes deben ser suprimidos una vez hayan dejado de ser útiles y pertinentes para la satisfacción de los fines que motivaron su creación. Durante el periodo de tiempo que los ficheros o archivos permanezcan en el equipo o soporte informático externo, deberá restringir el acceso y el uso de la información que obra en los mismos. ● El Usuario deberá restringir a terceros (familiares, amistades o cualesquiera otros) el acceso a los archivos o ficheros titularidad de la Organización y dispuesto a razón única de las funciones o tareas desempeñadas en la misma. Se establecerán medidas de protección adicionales que aseguren la confidencialidad de la información almacenada en el equipo cuando el Usuario del mismo así lo solicite o cuando se trate de datos de carácter personal que requieran de las medidas de seguridad establecidas por la legislación vigente.
Identificación y autenticación	● Las contraseñas de acceso al equipo, sistema y/o a la red, concedidos por la Organización, son personales e intransferibles, siendo el Usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida. ● Por cuestiones de seguridad no están permitidas prácticas como: ○ Emplear identificadores y contraseñas de otros Usuarios para acceder al sistema y a la red de la Organización. ○ Intentar modificar o acceder al registro de accesos. ○ Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros.
Política de usuarios de dispositivos locales	● Ubuntu ○ Los usuarios de dichos dispositivos requerirán siempre privilegios de administrador, ya que su trabajo requiere poder instalar y desinstalar software, y modificar parámetros de bajo nivel del sistema, como parte de sus tareas. ● Mac / Windows

	○ No se define una política de usuarios para estos dispositivos locales, puesto que esto podría limitar su agilidad en el trabajo del día a día.

5.2. Uso de la red corporativa

La red corporativa es un recurso compartido y limitado. Este recurso sirve no solo para el acceso de los Usuarios internos de la Organización a la Intranet o Internet, sino también para el acceso a las distintas aplicaciones informáticas corporativas y la comunicación de datos entre sistemas de tiempo real y explotación.

Por razones de seguridad, y con el fin de evitar riesgos, los Usuarios deben cumplir las siguientes medidas para el uso de la red corporativa:

Uso de internet	● La utilización de Internet por parte de los Usuarios autorizados debe limitarse a la obtención de información relacionada con el trabajo que se desempeña, debiendo, por lo tanto, evitarse la utilización que no tenga relación con las funciones del puesto de trabajo de Usuario, o que pudiera conducir a una mejora en la calidad del trabajo desarrollado. ● Con la finalidad de proteger que los sistemas sean comprometidos por código malicioso y para prevenir el acceso a recursos web no autorizados, la organización no permite el acceso a las siguientes categorías: o Código malicioso, construcción de explosivos, drogas, pornografía, racismo, sectas, violencia. ● Y se recomienda no acceder a estas categorías salvo autorización expresa: o Anonimizadores, Hackers, Spyware. ● La Organización podrá controlar el uso de acceso a Internet proporcionado. ● La normativa completa sobre el uso de Internet puede consultarse en el ANEXO 2 del presente documento.
Uso del correo electrónico	● Se considera el correo electrónico como un instrumento básico de trabajo. ● El acceso al correo se realizará mediante una identificación consistente en un usuario y una contraseña. Dicha identificación

	deberá seguir las mismas directrices que las planteadas para el acceso a las aplicaciones. ● Los envíos masivos de información, así como los correos que se destinen a gran número de usuarios, serán sólo los estrictamente necesarios que puedan provocar un colapso del sistema de correo. ● No deberán abrirse anexos de mensajes ni ficheros sospechosos o de los que no se conozca su procedencia. ● La Organización se reserva el derecho de que el *Responsable de Seguridad* pueda revisar y controlar el uso correcto del correo electrónico corporativo. ● En caso de ausencia, baja temporal o definitiva, el *Responsable del Departamento* correspondiente podrá redireccionar su cuenta con la finalidad de continuar con el normal desarrollo de la actividad de la Organización. ● Incidencias: Los usuarios deberán comunicar a sus responsables directos sobre cualquier anomalía que detecten en su correo, así como de la apertura de un correo sospechoso o cualquier alerta generada por el antivirus. ● La Organización se reserva el derecho a revisar los ficheros LOG de los servidores, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la Organización como responsable civil subsidiario. ● La normativa completa sobre el uso del correo electrónico puede consultarse en el ANEXO 1 del presente documento.
Compartición de contenidos	● Se prohíbe el uso de programas de compartición de contenidos, habitualmente utilizados para la descarga de archivos de música, vídeo, etc.

5.3. Acceso a aplicaciones y servicios en la nube

Tanto el equipamiento informático como todos los recursos facilitados al usuario para la realización de las tareas relacionadas con su puesto de trabajo (tales como, aplicaciones, servicios en la nube, etc.) son propiedad de la Organización, por lo que deberá hacerse un uso diligente de los mismos. En este sentido, se le informa de que podrá revisarse la utilización que cada Usuario esté haciendo para el desempeño de su puesto de trabajo.

Los Usuarios deben cumplir las siguientes medidas de seguridad establecidas por la Organización para el uso de aplicaciones y servicios corporativos:

Acceso a aplicaciones y servicios en la nube	● El acceso a las aplicaciones y servicios en la nube se realizará desde dispositivos proporcionados o aprobados por la empresa y que cumplan las medidas de seguridad establecidas por la organización.
Identificación y autenticación	● Tanto el acceso al ordenador como a las distintas aplicaciones corporativas o servicios será identificado (mediante usuario y contraseña, u otro mecanismo) y previamente autorizado por el responsable correspondiente.
Custodia de las contraseñas	● La custodia de la contraseña es responsabilidad del Usuario. Nunca debe utilizarse la cuenta de Usuario asignada a otra persona. ● No deben ser incluidas en correos electrónicos o en otros medios de comunicación electrónica junto con el identificador, ni comunicarlas por teléfono. ● No se deben escribir o almacenar contraseñas en texto claro o en formas fácilmente reversibles. ● Las contraseñas no deben anotarse, deben recordarse.
Renovación de las contraseñas	● Las contraseñas deben cambiarse periódicamente. Los Usuarios disponen de mecanismos para modificar la contraseña de acceso siempre que lo consideren conveniente. Esto garantiza el uso privado de las mismas.
Incidencias con las contraseñas	● Cuando se considere que la identificación de acceso se ha visto comprometida, se deberá comunicar al responsable correspondiente.
Cierre de sesiones y bloqueo del puesto de trabajo	● Al abandonar el puesto de trabajo deben cerrarse las sesiones, habilitar el protector de pantalla con bloqueo con contraseña, y apagar los equipos al finalizar la jornada

	laboral. Excepto en los casos en que el equipo deba permanecer encendido.
Aplicaciones y servicios permitidos	● Solo se utilizarán las aplicaciones y servicios en la nube aprobados por la organización.
Almacenaje, descarga y compartición de contenido	● Se prohíbe el almacenaje, descarga y difusión del contenido de la organización en las aplicaciones o servicios en la nube.
Privacidad y protección de datos	● Se cumplirá con las políticas de privacidad y protección de datos de la organización al utilizar aplicaciones y servicios en la nube. En caso de duda se consultará con el responsable correspondiente.

5.4. Acceso y tratamiento de datos personales

Regulación. NPAW, al ser una empresa con sede en España, está obligada a 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y de la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales.

Obligaciones. Dado que esta normativa trata de salvaguardar un derecho fundamental, mediante la adopción de diferentes medidas de seguridad, técnicas y organizativas, el Usuario, que accede y trata información de carácter personal en el desempeño de las funciones y tareas, deberá atender a las siguientes obligaciones:

Deber de secreto	● Guardar el necesario secreto respecto a cualquier tipo de información de carácter personal, conocida en función del trabajo desarrollado, incluso una vez concluida la relación que le une con la Organización.

Contraseñas	• Las contraseñas de acceso al sistema informático son personales e intransferibles, siendo el Usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida. • Queda prohibido, asimismo, emplear identificadores y contraseñas de otros Usuarios para acceder al sistema informático. • Los usuarios deben utilizar contraseñas seguras. Se entiende que una contraseña es robusta cuando posee, al menos, 8 caracteres (compuestos por letras mayúsculas y minúsculas, dígitos y signos especiales), evitando que la contraseña obtenida sea una palabra de un diccionario, una fecha o, de alguna manera, esté relacionada con el usuario (NIF, nombres propios y apellidos, nombres de mascotas, nombres de ciudades o países, nombres de personajes famosos, deportistas, etc.). Para evitar la problemática derivada de la necesaria memorización de las contraseñas, un mecanismo útil suelen ser los llamados acrósticos, que consisten en seleccionar un carácter de cada palabra de una frase conocida y fácilmente memorizable. Por ejemplo, la frase: “Mi nombre es Napoleón Bonaparte. Tengo 36 años.”, puede generar la siguiente contraseña: MneNB.T36a.
Bloqueo del puesto	• Bloquear la sesión del Usuario en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos de otras personas al equipo informático. Esto, sobre todo, deberá tenerse en cuenta, por parte del personal que esté en atención al público o comparta oficina con otros usuarios o no cierre la puerta de su despacho.
Almacenamiento de archivos	• Guardar todos los ficheros que contengan datos de carácter personal empleados por el Usuario, en el espacio de la red informática habilitado por la Organización a fin de facilitar la realización de las

	copias de seguridad o respaldo y proteger el acceso frente a personas no autorizadas.
Manipulación de los archivos	● Únicamente las personas autorizadas en función de su puesto de trabajo, podrán introducir, modificar o anular los datos personales contenidos en los ficheros.
Ficheros temporales	● Ficheros temporales son aquellos en los que se almacenan datos de carácter personal, generados a partir de un fichero general para el desarrollo o cumplimiento de una tarea/s determinada/s. ● Los ficheros temporales deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación, y mientras estén vigentes, deberán ser almacenados en la carpeta habilitada en la red informática, o de forma que puedan ser fácilmente localizados.
Correo electrónico	● No utilizar el correo electrónico (corporativo o no) para el envío de información de carácter personal especialmente sensible (esto es, salud, ideología, religión, creencias, origen racial o étnico). Este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información no sea inteligible ni manipulada por terceros.

Violaciones de seguridad de datos personales	● Entre otras acciones, tienen la consideración de violaciones de seguridad de datos personales las siguientes: ○ Pérdida de contraseñas de acceso a los Sistemas de Información. ○ Uso indebido de contraseñas. ○ Acceso no autorizado de usuarios a ficheros excediendo sus perfiles. ○ Pérdida de soportes informáticos o documentos en papel con datos de carácter personal. ○ Pérdida de datos por mal uso de las aplicaciones. ○ Ataques a la red. ○ Infección de los sistemas de información por virus u otros elementos dañinos. ○ Fallo o caída de los Sistemas de Información, etc. ○ Documentos que se hallen en papeleras con datos personales. ● Se deberán comunicar las violaciones de seguridad de datos personales de las que tenga conocimiento, que puedan afectar a la seguridad de los datos personales, de acuerdo al procedimiento establecido. Esto resulta también de aplicación a la información en papel.

Soportes informáticos (*pendrives* y discos duros externos, CDs, DVDs, etc.)	• No está permitida la salida de soportes que contengan datos personales fuera de los locales de la Organización si no está expresamente autorizada. • No está permitido el uso de unidades de almacenamiento de la información externas para uso privado como por ejemplo pendrives, discos duros externos, DVD-R, etc. • En caso de necesitar desechar un soporte que contenga datos personales, se entregará al departamento de sistemas que destruirá mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

5.4.1. Tratamiento de Datos Personales en Papel

En cuanto al tratamiento de datos personales en papel, el Usuario deberá observar las siguientes diligencias indicadas anteriormente con respecto a la confidencialidad de la información, acceso autorizado a la información en atención a las necesidades de su trabajo, gestión de soportes y documentos, trabajo fuera de las instalaciones de Barcelona. Asimismo, con carácter especial y únicamente de aplicación a los ficheros en papel, el Usuario deberá cumplir además con las siguientes diligencias:

Impresión de documentos	• La impresión de documentos en papel que contengan datos de carácter personal deberá restringirse al máximo y solo deberá hacerse en caso de ser necesario e indispensable.
Archivadores o dependencias	• Mantener debidamente custodiadas las llaves de acceso a los locales o dependencias, despachos, así como a los armarios,

	archivadores u otros elementos que contenga soportes o documentos en papel con datos de carácter personal. ● En caso de disponer de un despacho, cerrar con llave la puerta, al término de la jornada de trabajo o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.
Almacenamiento de documentos	● El archivo de la documentación se realizará siguiendo los criterios establecidos por la Organización, para garantizar su correcta conservación. ● Los soportes o documentos se archivarán en el lugar correspondiente, de modo que permitan una buena conservación, clasificación, acceso y uso de los mismos. ● No podrá acceder o utilizar los archivos pertenecientes a otros Departamentos, que compartan la sala o dependencia habilitada a archivo.
Custodia de documentos	● Cuando los documentos en soporte papel no se encuentren almacenados, por estar siendo revisados o tramitados, será la persona que se encuentre a su cargo la que deba custodiar e impedir, en todo momento, que un tercero no autorizado pueda tener acceso. ● Guardar todos los soportes o documentos que contengan información de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente, fuera de la jornada de trabajo. ● Asegurarse de que no quedan documentos impresos que contengan datos personales, en la bandeja de salida de la fotocopiadora, impresora o faxes. ● Se deberá mantener la confidencialidad de los datos personales que consten en los documentos depositados o almacenados en los escritorios, mostradores u otro mobiliario.
Traslado	● En los procesos de traslado de documentos deberán adoptarse medidas dirigidas para impedir el acceso o manipulación por terceros y, de manera que, no pueda verse el contenido, sobre todo, si hubiere datos de carácter personal. ● En caso de cambiar de dependencia, en el proceso de traslado de los documentos en soporte papel, se deberá realizar con el debido orden. Asimismo, se procurará mantener fuera del alcance de la vista de cualquier personal de la entidad, aquellos documentos o soportes en papel donde consten datos de carácter personal.

	● Si se envían a terceros ajenos a la Organización datos especialmente sensibles (esto es, salud, ideología, religión, creencias, origen racial o étnico) contenidos en soporte papel, se debe realizar en sobre cerrado y, en cualquier caso, tener presente que haya de efectuarse por medio de correo certificado o a través de una forma de correo ordinario que permita su completa confidencialidad.
Destrucción	● No tirar soportes o documentos en papel, donde se contengan datos personales, a papeleras o contenedores, de modo que pueda ser legible o fácilmente recuperable la información. ● A estos efectos, deberá ser siempre desechada o destruida mediante destructora de papel u otro medio que disponga la Organización.
Registro de accesos	● Se debe mantener un registro de accesos a la documentación (Ej.: datos sindicales, salud, etc., siempre y cuando vayan a ser utilizados por varios usuarios.
Incidencias	● Comunicar al Servicio de Sistemas y Comunicaciones las incidencias de seguridad de las que tenga conocimiento y que puedan afectar a la seguridad de los datos personales. ● Entre otros, tienen la consideración de incidencia de seguridad, que afecta a los ficheros en papel**,** los sucesos siguientes: ○ Pérdida de las llaves de acceso a los archivos, armarios y/o dependencias, donde se almacena la información de carácter personal. ○ Uso indebido de las llaves de acceso. ○ Acceso no autorizado de usuarios a los archivos, armarios y/o dependencias, donde se encuentran ficheros con datos de carácter personal. ○ Pérdida de soportes o documentos en papel, con datos de carácter personal. ○ Deterioro de los soportes o documentos, armarios o archivos, donde se encuentran datos de carácter personal.

5.5. Proceso disciplinario

El incumplimiento de las políticas corporativas y las normas contenidas en este documento se considera una transgresión de las obligaciones del empleado, susceptible de sanciones o la apertura de procedimientos disciplinarios, siempre en conformidad con la legislación y normativa locales. Las infracciones pueden acarrear consecuencias como advertencias, multas, suspensión o incluso despido, en función de la gravedad de la transgresión. La valoración de las consecuencias para el infractor y las medidas a adoptar serán tomadas de acuerdo con las normas que regulan la relación laboral entre la empresa y el empleado.

6. ANEXOS/FORMATOS

6.1. Anexo 1. Normas de uso del correo electrónico

6.1.1. Objetivo

El objetivo de la presente Norma es regular el acceso y utilización del correo electrónico (e-mail) por parte de los usuarios de los Sistemas de Información de la Organización, con el objeto de homogeneizar criterios dentro de sus unidades administrativas y definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios.

6.1.2. Alcance

Esta Norma es de aplicación a todo el ámbito de actuación de la Organización, y tiene origen en las directrices de carácter más general definidas en la Política de Seguridad de la Información.

La presente Norma será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la Organización, incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información propiedad de la Organización.

6.1.3. Cuerpo del documento

Concepto. El correo electrónico (e-mail) es un servicio de red para permitir a los usuarios de la Organización enviar y recibir mensajes. Junto con los mensajes también pueden ser enviados ficheros adjuntos.

Caracteres. Las características peculiares de este medio de comunicación (universalidad, bajo coste, anonimato, etc.) han propiciado la aparición de amenazas que utilizan el correo electrónico para propagarse o que aprovechan sus vulnerabilidades.

Especificaciones. La Organización, consciente de los problemas de seguridad y responsabilidad legal que ocasiona el uso del correo electrónico, dispone las siguientes especificaciones:

Responsabilidad	● Los usuarios serán responsables de todas las actividades realizadas con las cuentas de acceso y su respectivo buzón de correos provistos por la Organización. ● Los usuarios deberán ser conscientes de los riesgos que acarrea el uso indebido de las direcciones de correo electrónico suministradas por la Organización. ● Las cuentas de correo son personales e intransferibles. Salvo en casos puntuales -para los que deberá solicitarse y obtenerse la

	correspondiente autorización-, no se debe ceder el uso de la cuenta de correo a terceras personas, lo que podría provocar una suplantación de identidad y el acceso a información confidencial. ● Los mensajes de correo electrónico transmiten información en sus cabeceras (en principio ocultas) que indican datos adicionales del emisor, por lo que deben tenerse en cuenta posibles repercusiones (como daños a la imagen institucional) que podría acarrear una mala utilización de este recurso.
Uso aceptable	● Como norma general no se utilizará la herramienta de correo electrónico con fines ajenos al propio desarrollo de las actividades que cada usuario tiene encomendadas en la Organización. ● La utilización del correo electrónico por personal externo requiere la previa autorización por escrito de la Dirección. ● La forma y contenidos de los correos enviados por el usuario estarán alineados con las normas éticas y de cortesía marcadas por la Organización, y en ningún caso se enviarán correos ofensivos, amenazantes o de mal gusto. ● El usuario debe mantener ordenados y clasificados todos sus buzones y carpetas. Los correos inservibles deben ser eliminados, y todos los archivos adjuntos almacenados en el equipo o unidad de disco habilitada.
Usos no permitidos que implican un riesgo para la seguridad	● La difusión de contenido ilegal; como por ejemplo amenazas, código malicioso, apología del terrorismo, pornografía infantil, software pirata, o de cualquier otra naturaleza delictiva. ● El uso no autorizado de servidores propiedad de la Organización para el envío de correo personal. ● El envío masivo de correos publicitarios o de cualquier otro tipo que no guarde relación alguna con las necesidades de negocio de la Organización. Este hecho, además, puede llegar a ser interpretado como “spamming”. ● La divulgación, independientemente del formato en que se encuentren, de correos que revelen datos del directorio o de usuarios pertenecientes a la Organización, fuera de los límites laborales establecidos por la misma. ● En el caso de se requiera enviar un mensaje de correo electrónico a varios destinatarios, se utilizará preferentemente el campo CCO (copia oculta) para introducir las direcciones de correo de los

	destinatarios, con excepción de aquellos mensajes en los que necesariamente se requiera la identificación de todos los destinatarios para confirmar que han sido informados.
Diligencia	● Los archivos adjuntos recibidos serán analizados por las herramientas antivirus antes de ser abiertos o ejecutados. Los correos sospechosos o de dudosa procedencia no serán abiertos, y menos aún los archivos adjuntos que contengan. Su eliminación debe ser inmediata. Gran parte del código malicioso suele insertarse en ficheros adjuntos, ya sea en forma de ejecutables (.exe, por ejemplo) o en forma de macros de aplicaciones (Word, Excel, etc.). ● No emplear el correo electrónico como medio de comunicación para enviar o recibir información confidencial o que contenga datos de carácter personal de nivel alto (datos de salud, ideología, afiliación sindical, religión, creencias, origen racial, vida sexual, violencia de género, fines policiales). Únicamente, y en aquellos casos en los que sea estrictamente necesario, se utilizará este medio, en cuyo caso, se enviará con las medidas de seguridad apropiadas para cada tipo concreto de información mediante la utilización de un software de cifrado, previa autorización expresa del responsable de seguridad. ● En la medida de lo posible, desactivar la vista previa. Utilizar la vista previa para los correos de la bandeja de entrada comporta los mismos riesgos que abrirlos. Del mismo modo, limitar el uso de HTML. El código malicioso puede encontrarse fusionado con el código HTML del mensaje. Desactivar la visualización HTML de los mensajes ayuda a evitar que el código malicioso se ejecute.
Incidencias	● Los usuarios deberán comunicar a sus responsables directos sobre cualquier anomalía que detecten en su correo, así como de la apertura de un correo sospechoso o cualquier alerta generada por el antivirus.
Monitorización	● La Organización se reserva el derecho a revisar los ficheros LOG de los servidores, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la Organización como responsable civil subsidiario.

6.2. Anexo 2. Normas de uso de internet

6.2.1. **Objetivo**

El objetivo de la presente Norma es regular el uso de internet por parte de los usuarios de los Sistemas de Información de la Organización, con el objeto de homogeneizar criterios dentro de sus unidades administrativas y definiendo unas reglas de uso que deberán ser conocidas y observadas por todos los usuarios.

6.2.2. **Alcance**

Esta Norma es de aplicación a todo el ámbito de actuación de la Organización, y tiene origen en las directrices de carácter más general definidas en la Política de Seguridad de la Información.

La presente Norma será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la Organización, incluyendo el personal de organizaciones externas, cuando sean usuarios o posean acceso a los Sistemas de Información propiedad de la Organización.

6.2.3. **Cuerpo del documento**

Con carácter general, los usuarios de la Organización disponen de acceso a Internet como herramienta de productividad y conocimiento, así como de mejora de los sistemas de trabajo y búsqueda de información. Esta herramienta es propiedad de la Organización, la cual se reserva el derecho de conceder o anular dichos accesos conforme a los criterios que crea convenientes.

Es necesario garantizar un uso adecuado de los recursos informáticos de acceso a Internet, por los siguientes motivos:

- Seguridad: debido al riesgo de infección por software dañino (virus, troyanos, etc.).
- Volumen del tráfico externo de datos: garantizando que el acceso a contenidos necesarios para la actividad profesional no se vea perjudicado por el tráfico generado por contenidos no vinculados con las competencias de la Organización.
- Volumen del tráfico interno de datos: como consecuencia de contenidos descargados de la Web y su posterior almacenamiento. Esta situación aconseja también regular el tipo de ficheros cuya descarga y almacenamiento está permitido.
- Ética: es ineludible el compromiso que la Organización debe mantener con la sociedad, a la hora de vetar el acceso a contenidos que pudieran ser poco éticos, ofensivos o delictivos.

Responsabilidad	● Internet es un servicio que Nice People At Work pone a disposición de su personal para uso estrictamente profesional. ● Los usuarios son los únicos responsables de las sesiones iniciadas en Internet desde sus terminales de trabajo, y se comprometen a acatar las reglas y normas de funcionamiento establecidas en la presente Normativa. ● El acceso a Internet por personal externo requiere la previa autorización por la Dirección.
Monitorización	● La Organización se reserva el derecho a filtrar el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios propiedad de la Organización, así como a monitorizar y registrar los accesos realizados desde los mismos. En caso de que un usuario considere necesario acceder a alguna dirección incluida en una de las categorías filtradas, se pondrá en contacto con su responsable directo para que este gestione el acceso correspondiente.
Usos no permitidos que implican un riesgo para la seguridad	● Se prohíbe expresamente el acceso, la descarga y/o el almacenamiento en cualquier soporte, de páginas con contenidos ilegales, dañinos, inadecuados o que atenten contra la moral y las buenas costumbres y, en general, de todo tipo de contenidos que incumplan las normas éticas y de cortesía de la Organización. ● No se permite el almacenamiento en los equipos de archivos que violen la legislación vigente relativa a Propiedad Intelectual. Los usuarios deberán respetar y dar cumplimiento a las disposiciones legales de derechos de autor, marcas registradas y derechos de propiedad intelectual de cualquier información visualizada u obtenida mediante Internet haciendo uso de los recursos informáticos o de red de la Organización. ● Se prohíbe el uso de Internet para obtener o distribuir material violento o pornográfico, o para obtener o distribuir material incompatible con los valores de la Organización.
Incidencias	● Cualquier incidente de seguridad relacionado con la navegación por Internet, deberá ser comunicado sin demora al responsable directo oportuno

6.3. Anexo 3. Teletrabajo

6.3.1. Objetivo

El objetivo del presente documento es describir las circunstancias especiales que deben considerarse por parte del empleado/usuario en el desempeño de sus actividades laborales sobre un entorno de teletrabajo.

6.3.2. Alcance

Este protocolo pretende ayudar y asesorar al empleado del entorno de teletrabajo para que aplique unas pautas de comportamiento y permita, de esta forma, gestionar los riesgos que este contexto laboral puede generar sin las debidas precauciones.

6.3.3. Cuerpo del documento

6.3.3.1. Seguridad física de los dispositivos

Vigilancia y control del dispositivo físico. Los dispositivos móviles facilitados por la organización deben estar vigilados y bajo control para evitar extravíos o hurtos que comprometan la información almacenada en ellos o que pueda extraerse de ellos. En los desplazamientos en avión, este tipo de equipamiento no debe facturarse y deberá viajar siempre con el usuario.

6.3.3.2. Acceso remoto a los sistemas corporativos

Conexiones remotas. Las conexiones remotas a los sistemas de la organización se deben adecuar a las directrices establecidas por cada departamento. Se utilizarán los canales de comunicación para el establecimiento de VPN que se indiquen con las configuraciones de seguridad que se hayan establecido como necesarias.

- Departamento de QA: Acceso a la VPN de la oficina para poder realizar test de dispositivos en los cuales la IP pública habilitada por parte del cliente es la corporativa.
- Departamento de Sistemas y desarrollo: Acceso a la VPN de sistemas (openVPN) para el acceso a los dispositivos conectados a la IP interna del datacenter.

Bloqueo de sesión. El equipo debe tener activo el protector de pantalla con contraseña, para que quede bloqueado cuando no se utilice. El trabajador/colaborador no permitirá el uso del mismo por parte de otras personas.

6.3.3.3. Gestión de la información almacenada en los dispositivos

Acceso a los datos. Se debe evitar el acceso a la información y a los equipos por parte de terceras personas externas a la organización, como pudieran ser miembros del entorno familiar.

Copias de seguridad. Siempre que sea posible, la información corporativa debe quedar almacenada en los recursos de red corporativos, evitando utilizar los discos locales del equipo.

6.3.3.4. Conexiones a redes inalámbricas

Redes wifi. En caso de tener que conectarse a la red mediante una red wifi que no garantice la seguridad, debemos buscar los mecanismos necesarios para que la comunicación se realice de la forma más segura posible. Debemos ser especialmente cuidadosos con las redes públicas desprotegidas y establecer medidas que nos ayuden a evitar problemas como el robo de credenciales, manipulación de nuestra información de trabajo, etc. Para hacer más segura la conexión en este tipo de redes debemos establecer medidas como las siguientes:

- Desconfiar de las redes wifi públicas o gratuitas.
- Utilizar los canales cifrados seguros de comunicación que se proporcionen: VPN o algún otro tipo de cifrado punto a punto, como los sitios web con protocolos SSL y certificados.
- Desconectar la wifi de los dispositivos cuando no la estemos utilizando.
- Preferentemente, hacer uso de redes 3G o 4G antes que de redes wifi inseguras.

6.3.3.5. Incidentes de seguridad vinculados a estos dispositivos

- Pérdida o robo. Ante la pérdida o robo de un dispositivo móvil propiedad de la Organización, el empleado debe notificarlo a su responsable directo.
- Acceso no autorizado. Si un empleado conoce o sospecha que un tercero ha tenido acceso a sus dispositivos móviles o sus credenciales de acceso remoto porque conoce las claves de acceso o ha podido eludir las medidas de seguridad establecidas, deberá notificarlo a su responsable directo en la mayor brevedad posible.

REFERENCIAS

- UNE-ISO/IEC 27001:20022, Control A.5.10 Uso aceptable de la información y otros activos asociados.
- NO-LEGISLACIÓN Y NORMATIVA APLICABLE
- Procedimiento Disciplinario