Universidad de Navarra

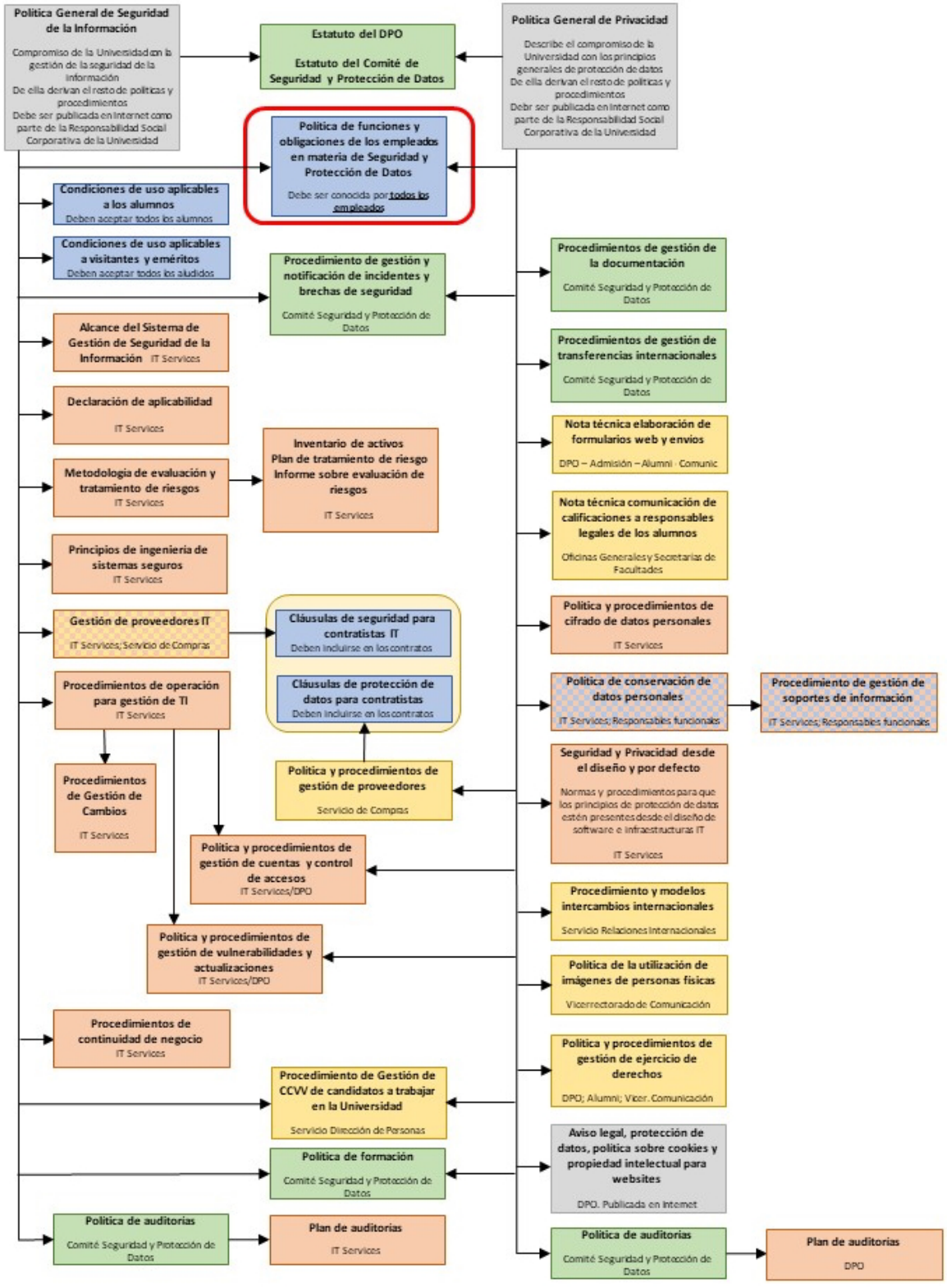
FUNCIONES Y OBLIGACIONES DE LAS PERSONAS TRABAJADORAS EN MATERIA DE SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN Y DATOS PERSONALES

Conforme a la norma UNE ISO/IEC 27001:2015
Conforme a la norma ISO/IEC 27701:2019

Versión 15g2

UNIVERSIDAD DE NAVARRA
CIF: R3168001J
Campus Universitario, S/N. Edificio Central. 31080, Pamplona

Mapa de políticas en materia de seguridad de la información y protección de datos personales 20/01/22



INDICE

1. OBJETO Y ÁMBITO DE APLICACIÓN. NATURALEZA DEL SISTEMA DE INFORMACIÓN DE LA UNIVERSIDAD DE NAVARRA. ASUNCIÓN DE LA POLÍTICA

El objeto de esta política es:

- Regular aspectos básicos de la normativa y condiciones de uso del Sistema de Información de la Universidad de Navarra y aquellas entidades que colaboran en el desarrollo de sus actividades relacionadas en https://www.unav.edu/proteccion-de-datos#entidades (en adelante referidas de forma conjunta como "la Universidad de Navarra" o "la Universidad").
- Definir las responsabilidades en cuanto a su utilización por las Personas Trabajadoras de la Universidad o las referidas entidades, insistiendo especialmente en lo que afecta a los datos personales y en el uso de las herramientas y dispositivos de comunicación y de gestión de la información que la Universidad pone a disposición de las Personas Trabajadoras.
- Proporcionar a las Personas Trabajadoras indicaciones necesarias para mejorar la seguridad de la información y la protección de los datos personales.

A los efectos de esta Política, se denomina "Sistema de Información de la Universidad de Navarra" o, abreviadamente, "Sistema de Información" al conjunto de software, hardware, infraestructuras y datos que dan soporte informático y de telecomunicaciones a los procesos de la Universidad de Navarra, incluyendo la documentación existente o que se pueda generar a partir de ésta, se encuentre en soporte automatizado o no.

Esto incluye, entre otros:

- Los dispositivos informáticos (ordenadores, tabletas, smartphones, impresoras, fotocopiadoras, periféricos, servidores, soportes de almacenamiento de datos, etc.);
- El software asociado (sistemas operativos, software base, aplicaciones específicas instaladas en los dispositivos o accesibles a través de Internet, etc.);
- Los servicios en red (cuentas de acceso, correos electrónicos, carpetas personales o compartidas, Internet, Intranet, servicios en la nube, videoconferencia, etc.);
- Cualquier información en cualquier formato, incluido el formato en papel, que se trate en los elementos anteriores (contenido de los archivos informáticos, bases de datos, etc.), o que se pueda generar a partir de ésta, o esté relacionada con ella (listados, cartas, nóminas, etiquetas con datos personales, etc.).

Todos los elementos del Sistema de Información de la Universidad de Navarra son propiedad de la Universidad, que los pone a disposición de las Personas Trabajadoras y usuarios autorizados para el desarrollo del objeto de su prestación laboral y de los fines de la Universidad de Navarra (la docencia, la investigación, la atención sanitaria, las tareas administrativas, actividades museísticas, culturales e iniciativas sociales), así como las actividades o tareas auxiliares relacionadas con el funcionamiento de los servicios ofrecidos por la Universidad y sus distintos centros.

Los elementos del Sistema de Información deben ser considerados como herramientas de trabajo de la Universidad, por lo que su uso debe estar destinado a fines profesionales y al cumplimiento de las prestaciones para las que fue contratada la Persona Trabajadora, debiendo utilizarse de forma adecuada a su naturaleza y a dichos fines profesionales.

En la medida en que es una herramienta de producción y a través de ella se cumple la prestación profesional, **la Universidad se reserva el derecho de acceder a la información que contenga por motivos de seguridad, necesidades de negocio, cese laboral, baja o vacaciones de la Persona Trabajadora,**

situaciones de urgencia o cualquier otra causa razonable, así como de eliminar la información que considere conveniente.

Por ello, la Persona Trabajadora **no debe almacenar información privada en el Sistema de Información** de la Universidad.

Además de esta Política de Funciones y Obligaciones de las Personas Trabajadoras en materia de Seguridad y Protección de Datos, puede haber normas específicas adicionales para el uso de algunos elementos del Sistema de Información.

El acceso y la utilización del Sistema de Información de la Universidad de Navarra implica que la Persona Trabajadora ha asumido íntegramente y sin reservas la presente Política.

Queda prohibida toda utilización del Sistema de Información que suponga la violación de la presente política y/o de la buena fe contractual que debe presidir en todo momento la relación profesional suscrita con las Personas Trabajadoras. En los casos más graves y culpables, dicha violación podrá comportar consecuencias de índole laboral y/o disciplinaria.

Con relación a las obligaciones, prohibiciones y/o limitaciones sobre la facultad de control de la Universidad en el uso de elementos del Sistema de Información, facilitados a las Personas Trabajadoras para el cumplimiento de las prestaciones para las que fueron contratados, la Universidad de Navarra respetará y observará lo dispuesto en la normativa aplicable vigente en cada momento.

Todos los elementos del Sistema de Información de la Universidad de Navarra de los que disponga una Persona Trabajadora para el cumplimiento de sus obligaciones laborales, incluyendo la información y datos, deben ser devueltos a la Universidad cuando finalicen los contratos laborales que vinculan a ambos.

Sin perjuicio de lo anterior, la Universidad ha dispuesto el acceso al Sistema de Información de la Universidad de Navarra a distintos colectivos que, pese a no tener una relación laboral con la Universidad, colaboran con sus fines de diversa forma. Entre ellos están los jubilados, profesores eméritos, profesores colaboradores y otros externos. Estos colectivos quedan fuera del ámbito de aplicación de esta política, en tanto que tienen una específica para regular su situación.

2. CONFIDENCIALIDAD

La Persona Trabajadora se compromete a preservar, en todo momento, la confidencialidad de la información a la que tenga acceso en el marco de la relación laboral, y, en consecuencia, se obliga a no revelar a terceros ni a divulgar públicamente, ni durante la vigencia de la relación, ni posteriormente, tras su expiración o rescisión por cualquier causa, ninguna información relativa a datos personales, expedientes, historias clínicas, contratos, procedimientos, especificaciones, procesos, programas, datos o información técnica, comercial, financiera, etc., perteneciente a la Universidad de Navarra, que pueda conocer por la relación laboral establecida entre ambos.

La revelación de información confidencial, especialmente en el caso de datos personales de los que es Responsable la Universidad, podría constituir, en los casos graves y culpables, una infracción laboral objeto de expediente disciplinario y, en algunos casos, un delito penal.

3. CONDICIONES GENERALES DE USO DEL SISTEMA DE INFORMACIÓN DE LA UNIVERSIDAD DE NAVARRA

La Persona Trabajadora utilizará el Sistema de Información de la Universidad de Navarra correctamente, de acuerdo con la legislación vigente, la presente Política y las normas de uso particulares de los elementos del Sistema de Información que utilice, si las hubiera, evitando cualquier actuación ilícita o lesiva de derechos o intereses de la Universidad de Navarra o de terceros.

Queda prohibido destruir, alterar, inutilizar o dañar de cualquier otra forma los datos, programas, documentos electrónicos o no automatizados, o cualquier otro elemento del Sistema de Información de la Universidad de Navarra o de terceros, pudiendo constituir estos actos un delito de daños, previsto en el artículo 264.2 del Código Penal.

Asimismo, se compromete a profesar una actitud y a utilizar un lenguaje leales y respetuosos en las comunicaciones con otros Trabajadores y con terceros, tanto en espacios públicos como privados, y a no transmitir o difundir opiniones o contenidos ilegales, difamatorios, ofensivos o que atenten contra los fines propios de la Universidad de Navarra, su Ideario o la dignidad de las personas.

La Persona Trabajadora reconoce y acepta que todos los derechos de propiedad industrial e intelectual de las aplicaciones software del Sistema de Información pertenecen a la Universidad de Navarra o a terceros que han cedido a ésta sus derechos, y sólo está autorizado para su uso en las actividades propias de la Universidad. Cualquier otro uso estará sujeto a la previa y expresa autorización otorgada por la Universidad de Navarra o el tercero titular de los derechos afectados.

4. NORMATIVA ESPECÍFICA SOBRE LAS CUENTAS DE USUARIO

Para desarrollar las tareas diarias, se asigna a cada Persona Trabajadora una cuenta con unas claves de acceso (generalmente un nombre de usuario y una contraseña) que deberá introducir para acceder a su equipo informático y a la mayoría de las aplicaciones. Además, es posible que se asignen claves de acceso específicas o medidas de seguridad adicionales para el uso de algunas aplicaciones concretas.

Las contraseñas deben tener las siguientes características:

1. Estar formadas por al menos 12 caracteres y 64 como máximo. La contraseña es más segura cuantos más caracteres tenga, siendo una buena práctica utilizar frases de contraseñas o *passphrase*.
2. Estar formada por letras (salvo ñ) mayúsculas y minúsculas, y números. Se recomienda incluir al menos un carácter especial del tipo ./+-\":$%*.
3. La contraseña no podrá contener el nombre de usuario.
4. La contraseña caducará a los 12 meses y no se podrá repetir.

La contraseña debe ser memorizada. En caso de ser anotada, se mantendrá oculta (por ejemplo, no se emplearán papeles pegados a los equipos ni agendas o calendarios de mesa).

Las contraseñas son personales e intransferibles. No pueden ser facilitadas a terceros (ni siquiera al responsable de la Persona Trabajadora o a quien le sustituya durante periodos de baja o vacaciones).

Las contraseñas de acceso a los sistemas informáticos de la Universidad no deben utilizarse en ningún otro servicio al que tenga acceso la Persona Trabajadora (redes sociales, suscripciones, sitios de comercio electrónico, etc.)

Una forma de generar contraseñas sencillas de recordar, pero eficaces, es el uso de acrónimos de frases. Por ejemplo: "Mi hija Conchita come 2 veces más que Pedro, pero menos que María": MhCc2v+qPp-qM

Las contraseñas pueden cambiarse en la página web: https://www.unav.edu/web/it/cuentas-y-claves

Si la Persona Trabajadora sospecha que alguien está utilizando sus claves de acceso, debe comunicarlo inmediatamente al Centro de Atención al Usuario (CAU) de IT Services (teléfono interno 802992) y al Delegado de Protección de Datos *(Data Protection Officer)* de la Universidad (dpo@unav.es).

El acceso al Sistema de Información se bloqueará al terminar la relación laboral con la Universidad, y se eliminarán los datos asociados a la cuenta, incluyendo el buzón de correo electrónico.

Se exceptúan las personas jubiladas, que podrán solicitar el mantenimiento del acceso a algunos servicios de por vida, así como investigadores con artículos científicos pendientes de publicación o situaciones similares, a los que podrá concederse acceso a ciertos servicios durante un tiempo limitado, previa aprobación del responsable de la investigación.

5. NORMATIVA ESPECÍFICA DE USO DEL CORREO ELECTRÓNICO CORPORATIVO

La Universidad de Navarra proporciona a las Personas Trabajadoras una cuenta o buzón individual de correo electrónico corporativo, de uso personal e intransferible, cuya dirección está formada por la inicial del nombre y el primer apellido, o una combinación similar, seguidos de "@unav.es", "@unav.edu", "@ceit.es", etc.

El buzón de correo corporativo es una herramienta de comunicación que la Universidad de Navarra pone a disposición de las Personas Trabajadoras **para fines relacionados con la actividad de la Universidad.** Por tanto, **no está permitido el uso particular del correo electrónico corporativo**, y las Personas Trabajadoras no deben transmitir, distribuir, almacenar, descargar, instalar, copiar, visualizar o enviar contenidos ajenos al desarrollo de su actividad profesional.

Por razones históricas, que provienen de la época en que el correo electrónico era una herramienta casi exclusiva de las universidades y centros de investigación, se viene tolerando un uso limitado para fines particulares, siempre que ello no atente contra los fines o la imagen de la Universidad, y no interfiera en la actividad ni afecte a la productividad de la Persona Trabajadora.

Sin embargo, la facilidad con que se puede obtener actualmente una cuenta de correo electrónico de calidad aconseja ir trasladando a cuentas personales la utilización particular que pudiera hacerse del correo corporativo, como una buena práctica para mejorar la seguridad de la información almacenada en ambas cuentas.

En cualquier caso, no están permitidas las siguientes prácticas:

- **Utilizar la cuenta corporativa para el desarrollo de actividades privadas de carácter profesional.**
- **Difundir contenidos contrarios a las leyes o que vulneren los derechos de terceros.** Por ejemplo, y entre otros, (i) la difusión de materiales que vulneren derechos de propiedad intelectual o industrial de terceros, (ii) la difusión de contenidos difamatorios, obscenos, violentos o amenazantes, (iii) la difusión

de mensajes xenófobos, racistas, sexistas o que realicen apología del terrorismo.

- **Realizar envíos masivos de correo** (por ejemplo, para información de actividades, novedades, invitación a eventos, etc.[1]), sin la autorización del Responsable Funcional de los datos (v 8.1 y 8.8).
- **Realizar comunicaciones comerciales no solicitadas**, reenviar mensajes en serie ("cadenas" de mensajes), o cualquier tipo de comunicación maliciosa o dañina que pueda incluir virus, troyanos, etc. o inducir a la instalación de éstos por desconocimiento o descuido del receptor del mensaje.
- **Divulgar información corporativa de uso interno**, confidencial o comercial de la Universidad o que viole los derechos de propiedad intelectual.
- Con carácter general, **no se permite a las Personas Trabajadoras redireccionar automáticamente los correos electrónicos recibidos en cuentas de correo corporativas a cuentas de correo no corporativas y viceversa**. En el caso de que una Persona Trabajadora necesite redireccionar una cuenta de correo, deberá antes solicitarlo motivadamente y recibir autorización por escrito de la Universidad.
- **Utilizar la cuenta de correo de otra Persona Trabajadora.**
- **Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o los archivos de otra persona.** Sin perjuicio de la capacidad de supervisión que puede realizar la Universidad para comprobar el uso del correo electrónico, que en todo caso se realizará tratando de preservar la intimidad de la Persona Trabajadora y su dignidad profesional tal y como se indica en el apartado siguiente, se informa de que estas actividades pueden constituir un delito penal de interceptación de las telecomunicaciones, previsto en el artículo 197 del Código Penal.
- **Imitar, sustituir o modificar** las señas de identidad de cualquier persona o su dirección de correo electrónico.
- **Suministrar a terceros listados de direcciones** de correo de Personas Trabajadoras, estudiantes, etc. sin conocimiento de éstos.
- En general, cualquier comportamiento que directa o indirectamente cause o pueda causar daño, alteración o errores en el funcionamiento adecuado de los servicios de correo electrónico de la Universidad, que contravenga las disposiciones legales vigentes, o que suponga un incumplimiento de las obligaciones derivadas de la relación profesional, especialmente de la lealtad y la buena fe contractual.

Las condiciones anteriores aplican análogamente a las cuentas y direcciones creadas para su uso colectivo en los departamentos, servicios u otros recursos de la Universidad.

5.1. ACCESO AL CORREO ELECTRÓNICO DE LA PERSONA TRABAJADORA

[1] Se pueden hacer envíos internos, por ejemplo, a las personas que trabajan en el mismo departamento, área o Servicio, siempre que sean pertinentes y no excesivos, es decir, que estén relacionados con la actividad del grupo o entorno de trabajo, tengan interés, en general, para esas personas, y su frecuencia no moleste. Si no, es mejor reducir el envío a quienes realmente puedan estar interesados.
También a grupos limitados de colegas profesionales de fuera de la Universidad, colaboradores externos en proyectos, etc. siempre que se cuente con la autorización de los destinatarios o el envío se enmarque en alguna actividad común que lo haga necesario. En este caso es muy importante que se pongan los destinatarios en "copia oculta" para no difundir direcciones de correo que otras personas nos han confiado, pero quizá no quieran que sean públicas

La Universidad de Navarra podrá acceder al buzón de correo de las Personas Trabajadoras para garantizar la integridad del Sistema de Información, realizar tareas de mantenimiento técnico o continuar con la actividad diaria en caso de bajas temporales o definitivas, periodos de vacaciones o situaciones de urgencia o excepcionales análogas, así como para comprobar el buen uso del correo electrónico por parte de las Personas Trabajadoras en cualesquiera otros supuestos previstos en la legislación vigente.

Las Personas Trabajadoras no deben facilitar su contraseña de acceso al correo a terceros o a compañeros de trabajo **bajo ninguna circunstancia**.

Cuando una Persona Trabajadora se ausente por más de cinco días laborables de su puesto de trabajo, por baja, vacaciones, etc., deberá colocar un aviso automático indicando los datos de contacto de la persona que le sustituye en sus funciones, cuando sea el caso.

En caso de baja definitiva o excedencia de la Persona Trabajadora sin derecho a reingreso, a solicitud del supervisor de la Persona Trabajadora, el personal de IT Services activará dicho aviso automático indicando que la cuenta no se encuentra operativa, y en su caso, los datos de contacto de quien le sustituye, permaneciendo activado dicho aviso por el tiempo que indique el responsable del departamento o servicio.

5.2. CONSERVACIÓN DE CORREOS ELECTRÓNICOS

Las Personas Trabajadoras conservarán aquellos mensajes de correo electrónico que contengan información, documentos de trabajo o comunicaciones con terceros de relevancia para la Universidad, siempre de conformidad con las instrucciones del responsable del departamento o servicio, e incluyendo sus anexos si los hay.

En caso de cambio de funciones, baja prolongada, terminación de la vinculación con la Universidad, o situaciones similares que lo aconsejen, deben transmitirlos a quienes les sucedan en sus funciones en la forma que indique la persona que supervise éstas.

El servicio de correo electrónico no proporciona copias de seguridad, es decir, no hay posibilidad de recuperar un buzón en el estado en el que se encontraba en un momento anterior concreto, aunque el propio usuario puede generalmente recuperar los mensajes borrados más recientemente. Por ello, se recomienda salvar los documentos más importantes y conservar los mensajes adecuadamente clasificados y ordenados según las instrucciones del responsable del departamento o servicio.

Dado que, como se ha señalado, las cuentas de correo electrónico son herramientas de trabajo destinadas a un uso profesional, la Universidad de Navarra **no asumirá ninguna responsabilidad sobre la información personal que pudieran contener los buzones de las Personas Trabajadoras**.

5.3. FIRMA Y AVISO LEGAL EN LOS CORREOS

Las Personas Trabajadoras deberán identificarse en los correos salientes con una firma que siga el siguiente estándar (el logotipo puede cambiar en función de la entidad en que trabaje):

Existe una aplicación para facilitar la confección de la firma, a la que se puede acceder desde https://portaldelempleado.unav.edu/servicios-centrales.

Todos los mensajes tendrán que incluir el siguiente aviso después de la firma (generalmente, se ocupa de añadirlo de forma automática el propio servidor de correo electrónico):

"Este mensaje puede contener información confidencial. Si usted no es el destinatario o lo ha recibido por error, por favor, bórrelo de sus sistemas y comuníquelo a la mayor brevedad al remitente. Los datos personales incluidos en los correos electrónicos que intercambie con el personal de la Universidad de Navarra podrán ser almacenados en la libreta de direcciones de su interlocutor y/o en los servidores de la Universidad durante el tiempo fijado en su política interna de conservación de información. La Universidad de Navarra gestiona dichos datos con fines meramente operativos, para permitir el contacto por email entre sus trabajadores y terceros. Tiene derecho a acceder, rectificar y suprimir los datos, entre otros que se relacionan en la Política de Privacidad la Universidad de Navarra accesible en: https://www.unav.edu/aviso-legal"

6. USO DE INTERNET Y DE LA RED CORPORATIVA

6.1. NORMA GENERAL

La Universidad pone a disposición de las Personas Trabajadoras un acceso a Internet y una red corporativa que forman parte del Sistema de Información, y **sólo deben utilizarse para fines profesionales** relacionados con la actividad laboral que se desempeñe.

La descarga de Internet, instalación, reproducción, uso o distribución de aplicaciones **cuya procedencia y seguridad se encuentren debidamente contrastadas**, está permitida siempre que la Persona Trabajadora tenga constancia cierta de disponer de licencia para ello. En caso de duda sobre este aspecto, conviene consultar a IT Services.

La descarga y utilización de cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, está permitida siempre que la Persona Trabajadora tenga constancia cierta de disponer de la oportuna licencia o excepción para ello, conforme a la legislación vigente en la materia.

No están permitidas, además de las conductas ya indicadas con carácter general en la presente Política, las siguientes acciones:

- Utilizar el sistema para intentar acceder a áreas restringidas del Sistema de Información o que no hayan sido autorizadas expresamente a la Persona Trabajadora.
- Introducir voluntariamente programas, virus, macros o malware similar que puedan causar cualquier tipo de alteración en el Sistema de Información.

- Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad, en el Sistema de Información.

La Persona Trabajadora está obligada a utilizar la red corporativa e Internet sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de la Universidad o de terceros, o que puedan atentar contra la moral o las normas de cortesía y urbanidad que rigen en el ámbito físico y digital, así como contra las leyes, políticas y reglamentos que sean de aplicación.

Las Personas Trabajadoras **observarán la mayor diligencia en la descarga y apertura de links y archivos**, para intentar evitar la contaminación por *malware* del Sistema de Información o algunos de sus elementos, siguiendo en todo momento las indicaciones recibidas de IT Services de la Universidad.

La Universidad, para garantizar y velar por el cumplimiento de esta política, se reserva el derecho a bloquear la navegación por cualquier página de Internet que considere oportuna; el Sistema de Información mostrará un mensaje a la Persona Trabajadora en el caso en que sea bloqueada alguna página. Si algún Trabajador o Trabajadora considerase necesario para el desarrollo de su actividad profesional el acceso a alguna de las páginas bloqueadas podrá solicitar a IT Services el desbloqueo de la misma.

6.2. REGISTRO DE LOS ACCESOS A INTERNET. CLÁUSULA INFORMATIVA DEL TRATAMIENTO DE LOS DATOS PERSONALES: DATOS DE ACCESO A INTERNET

Las Personas Trabajadoras quedan informadas de que, **por razones técnicas, gestión del cumplimiento normativo y seguridad,** la Universidad de Navarra realiza un **registro** *(log)* **de los accesos a Internet efectuados** desde las redes internas de la Universidad, que contiene los siguientes datos: usuario, máquina, dirección IP, páginas visitadas, fecha y hora, tiempo de conexión, ancho de banda utilizado, tipología(s) de páginas visitadas, páginas bloqueadas, páginas permitidas.

Sólo se accederá a estos registros en caso de que haya indicios de alguna irregularidad relevante en relación con las finalidades mencionadas en las cláusulas informativas de dicho tratamiento, que se detallan en el apartado 13.4.

7. EQUIPOS INFORMÁTICOS

7.1. NORMAS GENERALES

Los equipos informáticos asignados a las Personas Trabajadoras **son herramientas de trabajo**, y serán utilizados según los procedimientos internos vigentes en cada momento, teniendo en cuenta los estándares establecidos por la Universidad.

No están permitidas, además de las indicadas con carácter general en la presente Política, las siguientes conductas:

- Instalar, a iniciativa propia de la Persona Trabajadora, cualquier programa o aplicación informática no relacionada directa o indirectamente con su actividad profesional o los fines de la Universidad de Navarra, de la que no se disponga de licencia, o cuya procedencia y seguridad no se encuentren debidamente contrastadas. En caso de duda se consultará a IT Services para que pueda confirmar la existencia de licencia y/o valorar la seguridad de la aplicación. **La instalación de software cuando se tenga conciencia cierta por parte de la Persona Trabajadora de que no se encuentra**

debidamente licenciado (coloquialmente denominado "pirata"), es una conducta ilícita que puede conllevar responsabilidades penales y civiles, además de poner en riesgo evidente tanto los equipos informáticos como la información que contienen.

- Instalar en los equipos certificados digitales que puedan utilizarse para representar a la Universidad de Navarra, sin el debido apoderamiento notarial que lo permita o la autorización de la autoridad universitaria competente, según el caso.

La Persona Trabajadora queda informada de lo siguiente:

- **El personal de IT Services puede acceder a los equipos informáticos, físicamente o en modo remoto, para realizar tareas de mantenimiento, control de su uso, reparación y vigilancia del cumplimiento de políticas.**
- **La Universidad de Navarra podrá acceder a los equipos que utiliza su personal** para garantizar la seguridad del Sistema de Información o continuar con la actividad diaria en caso de bajas temporales o definitivas, periodos de vacaciones o situaciones de urgencia o excepcionales análogas, así como en cualesquiera otros supuestos previstos en la legislación vigente, incluida la adopción de medidas disciplinarias; en todo caso el acceso se realizará con la mayor de las cautelas para garantizar la intimidad de quien utiliza del equipo.
- Los equipos pueden ser reasignados a otro miembro del personal, según disponibilidad y necesidades de la Universidad.
- **La Universidad de Navarra no asume ninguna responsabilidad en caso de pérdida, deterioro, destrucción o acceso a documentos privados del personal almacenados en los equipos informáticos.**

Las Personas Trabajadoras tienen la obligación de archivar los documentos de trabajo elaborados en el desarrollo de sus funciones de forma ordenada y siguiendo los parámetros marcados por su Área o Departamento.

Se recuerda que **la responsabilidad de realizar las copias de seguridad del contenido de los equipos recae en la Persona Trabajadora.**

Se recomienda realizar copias periódicas del contenido de los ordenadores siguiendo las instrucciones que se indiquen desde IT Services.

Las Personas Trabajadoras deben trabajar utilizando las aplicaciones, programas y bases de datos centrales. Los equipos han sido configurados por IT Services con los accesos y programas necesarios para que cada uno o una realice su trabajo. Si fueran necesarios otros accesos o programas podrán dirigirse a IT Services para solicitar el acceso. **Los cambios en la configuración o la instalación de software adicional deberán ser solicitados a través de IT Services.**

8. OBLIGACIONES RELATIVAS A LAS OPERACIONES CON DATOS PERSONALES

8.1. DEFINICIONES

Se llama "dato personal" a cualquier información sobre una persona física identificada o identificable. Se considera persona identificable aquella cuya identidad pueda determinarse, directa o indirectamente, por ejemplo, mediante su nombre, un número de identificación como el DNI, datos de localización, un nombre de usuario en una aplicación en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona, como una fotografía, una grabación de su voz, etc.

Se denomina "Responsable Funcional" a aquella persona designada por la Universidad de Navarra para coordinar y supervisar las medidas de seguridad de los tratamientos de datos de carácter personal y velar por el cumplimiento de la normativa de protección de datos personales en un ámbito concreto, que puede ser una aplicación o fichero o conjunto de ellos. Por ejemplo, el Oficial Mayor es Responsable Funcional de los tratamientos relacionados con la Gestión Académica, los gerentes de los Servicios y Facultades son, habitualmente, los Responsables Funcionales de los tratamientos de datos personales que se hagan en sus respectivos ámbitos de actuación, etc.

Se conoce como "Delegado o Delegada de Protección de Datos" (DPD, o DPO, del inglés *Data Protection Officer*) a aquella persona física o jurídica, interna o externa a la Universidad de Navarra y designada por ésta, que, entre otras funciones, asesora a la Universidad y a las personas que trabajan en ella en relación con el tratamiento de datos personales, supervisa el cumplimiento de la normativa en dicha materia, y gestiona las consultas y reclamaciones de los interesados, así como la relación con las autoridades de control en materia de protección de datos personales. Actualmente, el Delegado de Protección de Datos de la Universidad es Enrique Reina Martín (Edificio Amigos, despacho S500, extensión 803983). Cualquiera puede consultarle cuando lo desee, preferiblemente por correo electrónico en la dirección dpo@unav.es.

8.2. Obligaciones generales de las Personas Trabajadoras en materia de protección de datos personales

Toda Persona Trabajadora que, en el ejercicio de su actividad en la Universidad, tenga acceso a datos personales, está obligado al cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (Reglamento General de Protección de Datos o RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

Entre los deberes de las Personas Trabajadoras se incluyen: el deber de mantener el secreto sobre los datos personales, custodiar los mismos para evitar su alteración, pérdida, tratamiento o acceso no autorizado, y la prohibición de comunicar los datos personales a otra persona o entidad salvo que se disponga previamente del consentimiento por escrito del interesado.

Las Personas Trabajadoras que acceden a datos personales o información confidencial están obligados a guardar secreto sobre los mismos, sea cual sea su función en la Universidad y el cargo que ocupen, incluso después de finalizada su relación con la Universidad de Navarra, salvo que sean requeridas a revelarlos por las autoridades públicas en el ejercicio de sus competencias.

A modo de ejemplo, deben evitarse prácticas como:

- Comentar con terceros datos de los expedientes de estudiantes y calificaciones, aunque sean familiares de éstos. Sólo los propios estudiantes y, cuándo estos lo consienten o en determinadas situaciones, sus padres y/o tutores, pueden tener acceso a dicha información.

- Utilizar aplicaciones de mensajería no aprobadas por la Universidad para intercambiar documentos confidenciales. En particular, **se recuerda que no se deben transmitir listados de** estudiantes**, calificaciones, etc. a través de *WhatsApp* o aplicaciones similares.**
- Tratar asuntos confidenciales o que afectan a personas en espacios públicos (cafetería, pasillos, etc.).

El modo preferente para la edición de documentos de trabajo de la Universidad, donde figuren datos personales o material susceptible de protección en materia de propiedad intelectual e industrial, es a través de las aplicaciones en la nube que la Universidad pone a disposición de su personal, como se detalla en otra sección (Google Workspace y Office 365).

Salvo que la Persona Trabajadora haya obtenido previamente una autorización para ello del Responsable Funcional de los datos, **no se podrán realizar copias de datos personales ni documentos confidenciales almacenados en el Sistema de Información de la Universidad de Navarra, por ejemplo, en móviles, portátiles, soportes extraíbles, sistemas personales de almacenamiento en la nube, etc. Esto afecta tanto a la información en formato electrónico como en formato papel.**

Está expresamente prohibido generar o almacenar en los equipos informáticos ficheros de datos personales sin obtener una autorización previa del Responsable Funcional de los datos.

En caso de **necesidad urgente para el cumplimiento de las obligaciones profesionales o fines de la Universidad**, si no es posible obtener a tiempo la autorización del Responsable Funcional, bastará con informar a éste de las operaciones que se van a realizar mediante un mensaje de correo electrónico.

Debe tenerse especial precaución con los ficheros temporales que contengan datos personales, cumpliendo estrictamente las mismas medidas de seguridad y privacidad y eliminándolos tan pronto como dejen de ser útiles.

Si hay posibilidad de ello, debe **cerrarse la puerta de los despachos** con llave al ausentarse temporalmente y al finalizar la jornada laboral, para evitar accesos no autorizados. Asimismo, deben custodiarse debidamente las llaves de los despachos, así como de los armarios, archivadores u otros elementos que puedan contener soportes o documentos con datos de carácter personal.

Está prohibido utilizar datos personales para fines privados o no relacionadas con las funciones asignadas en la Universidad. Queda expresamente prohibida la realización de copias de cualquier tipo de listado o fichero para uso particular o para su conservación fuera del Sistema de Información.

Debe evitarse comunicar datos personales o compartir documentación que los contengan con personas, incluso otro Personal de la Universidad, que no tengan autorizado el acceso.

Debe tenerse precaución al usar impresoras, fotocopiadoras, faxes, etc., para que no quede en ellos ningún documento que contenga datos de carácter personal. En términos generales, estos equipos, si son de uso colectivo, deben disponer de un sistema de acceso personalizado que requiera el uso de tarjeta identificativa, PIN individual o algún mecanismo semejante previo a la impresión de los trabajos. Si se encuentra algún documento en esta situación, debe entregarse al Responsable Funcional para que lo haga llegar a la persona adecuada u ordene su destrucción.

Deben atenderse las solicitudes de acceso, rectificación, supresión, oposición, limitación y portabilidad de datos personales hechas por cualquier persona, comunicándolas lo antes posible y siempre dentro de las primeras 24 horas desde la recepción de la solicitud de ejercicios de derechos, al Delegado de Protección de Datos, dpo@unav.es, para su tramitación conforme indique la legislación vigente, siguiendo diligentemente

las indicaciones de éste, pues estas solicitudes constituyen un **derecho de las personas cuyos datos custodia la Universidad.**

Para cualquier duda o comentario relacionada con la legislación y las obligaciones en materia de protección de datos, así como con su aplicación práctica, puede contactarse con el Delegado de Protección de Datos en la dirección e-mail indicada, dpo@unav.es, físicamente en el Edificio Amigos, despacho S500, o por teléfono en la extensión 803983.

8.3. NORMAS ESPECÍFICAS APLICABLES A ORDENADORES, ORDENADORES PORTÁTILES, TABLETAS, *SMARTPHONES* Y OTROS DISPOSITIVOS EQUIVALENTES

Los dispositivos asignados son herramientas de trabajo **para uso personal e intransferible del Trabajador o Trabajadora**, y no podrán ser compartidos con terceros (compañeros de trabajo, familiares, etc.).

Las Personas Trabajadoras deben custodiar dichos equipos con diligencia, para evitar que personas no autorizadas puedan acceder a la información contenida en ellos, especialmente a los datos personales.

Debe procurarse una orientación de la pantalla que impida a otras personas ver su contenido, así como bloquearla con un salvapantallas cuando no esté en uso.

Los dispositivos asignados deben ponerse a disposición de IT Services cuando sean requeridos para tareas de mantenimiento, actualización y comprobación del cumplimiento de esta política.

La Persona Trabajadora, al recibir el dispositivo, acepta que, en caso de pérdida o sustracción, el personal de IT Services pueda **bloquear o eliminar remotamente** la información que contenga. **Queda prohibido manipular o desconfigurar esta opción en el dispositivo**.

Las Personas Trabajadoras deberán utilizar los mecanismos de seguridad facilitados por la Universidad para evitar el robo o pérdida de los dispositivos portátiles o de la información que albergan y deberán cumplir con las instrucciones del fabricante; si no se dispone de éstas pueden solicitarse a IT Services.

Los dispositivos móviles, portátiles, smartphones, etc., que contengan datos personales **deben estar cifrados y protegidos por contraseña.** IT Services velará porque se cumpla esta disposición facilitando los medios adecuados para ello.

No está permitido el tratamiento de datos personales en dispositivos móviles que no sean propiedad de la Universidad, salvo autorización por parte del Responsable Funcional. En caso de necesidad urgente para el cumplimiento de las obligaciones profesionales o fines de la Universidad, si no es posible obtener a tiempo la autorización del Responsable Funcional, bastará con informar a éste de las operaciones que se van a realizar mediante un mensaje de correo electrónico.

Se puede acceder al correo electrónico y otros servicios informáticos de la Universidad en un ordenador u otro dispositivo móvil particular, siempre que se evite la descarga de documentos confidenciales o que contengan datos personales.

En los ordenadores o dispositivos que se compartan con otras personas, los navegadores y aplicaciones con acceso a recursos de la Universidad deben configurarse para que no guarden las contraseñas.

La pérdida o robo de un dispositivo móvil debe ser inmediatamente notificada a IT Services y, en caso de que contenga datos personales, al Responsable Funcional de los datos y al Delegado de Protección de Datos de la Universidad (dpo@unav.es).

Los dispositivos móviles deben ser devueltos a IT Services una vez dejen de utilizarse, para su destrucción segura o borrado seguro de su contenido y reasignación.

8.4. NORMAS ESPECÍFICAS APLICABLES A DISPOSITIVOS EXTRAÍBLES

A efectos de esta política, se consideran "Dispositivos Extraíbles" los discos duros USB, *pendrives* o memorias USB, CD, DVD y otros dispositivos equiparables.

Se recuerda a las Personas Trabajadoras que la utilización de este tipo de soportes genera importantes riesgos para la seguridad de los sistemas.

Como norma general, las Personas Trabajadoras no deben utilizar Dispositivos Extraíbles para almacenar datos de carácter personal, salvo que sea necesario para el desarrollo de su actividad profesional o los fines de la Universidad.

En el caso de que sea necesario almacenar datos de carácter personal en Dispositivos Extraíbles, se actuará siempre previa autorización del Responsable Funcional de los datos, siguiendo las siguientes normas:

- **Emplear sólo Dispositivos Extraíbles suministrados por la Universidad**.
- **Cifrar el Dispositivo**. IT Services informará de los mecanismos de cifrado oportunos para tales dispositivos.
- Utilizar el Dispositivo Extraíble exclusivamente para almacenar la información, sin mezclarla con otra información no confidencial o particular.
- Etiquetar el Dispositivo para facilitar su recuperación en caso de pérdida.
- Eliminar el contenido del Dispositivo una vez haya dejado de ser necesaria la información.

En caso de necesidad urgente para el cumplimiento de las obligaciones profesionales o fines de la Universidad, si no es posible obtener a tiempo la autorización del Responsable Funcional, bastará con informar a éste de las operaciones que se van a realizar mediante un mensaje de correo electrónico.

La pérdida o robo de un Dispositivo Extraíble que contenga datos de carácter personal o información confidencial debe ser inmediatamente notificada al Responsable Funcional de los datos, a IT Services y al Delegado de Protección de Datos *(Data Protection Officer)* de la Universidad (dpo@unav.es).

IT Services dispone de un protocolo de destrucción segura de Dispositivos Extraíbles. Las Personas Trabajadoras que tengan que desechar un Dispositivo Extraíble, deberán notificarlo a IT Services y seguir sus instrucciones.

8.5. ALMACENAMIENTO Y TRATAMIENTO DE DATOS EN INTERNET (NUBE O CLOUD)

Cuando estén permitidos, los tratamientos de datos personales, incluido el almacenamiento, así como de cualquier otra información relacionada con las actividades de la Universidad de Navarra, solamente podrán realizarse en los servicios *cloud* con los que la Universidad ha suscrito un contrato de encargo de tratamiento

de datos (actualmente, las **instancias de la Universidad de Google Workspace y Microsoft 365**, conocidas también como Google Apps y Microsoft Onedrive, respectivamente).

El uso de servicios de almacenamiento en la nube distintos de los citados en el párrafo anterior, entraña evidentes riesgos legales en cuanto a las condiciones de integridad, disponibilidad y confidencialidad de la información, el grado de cumplimiento de los requisitos de la legislación vigente en materia de protección de datos del proveedor del servicio, y la salvaguarda de la propiedad intelectual o industrial, si fuera el caso.

8.6. GESTIÓN DE DOCUMENTACIÓN EN SOPORTE PAPEL

Cada Persona Trabajadora es responsable de la adecuada custodia de la documentación en soporte papel que genere y/o utilice para el desarrollo de sus tareas.

El Servicio de Archivo General fijará con los distintos servicios, departamentos o áreas de la Universidad los criterios de archivo que permitan mantener la información en soporte papel organizada de forma lógica y faciliten la búsqueda de documentos y su destrucción transcurridos los plazos que correspondan.

Cada departamento o área establecerá una persona responsable de la gestión del archivo.

La documentación confidencial y/o que mantenga datos de carácter personal debe ser almacenada en armarios, cajoneras, archivadores, despachos o dependencias en general que dispongan de un sistema de cerrado con llave o mecanismo equivalente (por ejemplo, tarjeta electrónica, código, etc.).

A continuación, se señalan ejemplos de documentos que deben almacenarse en lugares cerrados:

- Información de solicitantes de admisión.
- Expedientes académicos y documentos en general de los estudiantes.
- Documentación que contenga comentarios y valoraciones de tutores sobre los estudiantes.
- Información relativa a donantes, patrocinadores y recaudación de fondos en general.
- Información relativa al personal de la Universidad (situaciones de baja, solicitud de permisos, nóminas, etc.), así como la información de candidatos a empleo.

En caso de no disponer de los archivadores, cajoneras, armarios, etc. necesarios para el adecuado archivo de los documentos confidenciales, la Persona Trabajadora debe solicitarlos a su supervisor para que haga el pedido correspondiente a través del Servicio de Compras.

Los documentos que contengan datos personales o confidenciales en soporte papel deben destruirse cuando ya no sean necesarios de forma segura, mediante una destructora de papel.

Salvo en los destinados específicamente a destrucción de papel, que estarán convenientemente señalizados para ello, se prohíbe depositar en papeleras o contenedores documentos que contengan datos de carácter personal y/o información confidencial (expedientes de estudiantes **o Personas Trabajadoras, listados de calificaciones, exámenes, fichas de** estudiantes**, etc.).**

No debe reutilizarse el papel por el dorso si contiene datos personales o información confidencial.

8.7. POLÍTICA DE "MESAS LIMPIAS"

Al finalizar la jornada laboral, o cuando se ausenten por un rato prolongado del lugar de trabajo, las Personas Trabajadoras dejarán su escritorio lo más despejado posible, evitando dejar a la vista documentos con información confidencial o datos personales.

8.8. ENVÍOS MASIVOS POR CORREO ELECTRÓNICO Y ORDINARIO

Como se ha indicado anteriormente, **no está permitido que las Personas Trabajadoras realicen envíos masivos** por correo electrónico u ordinario (postal) sin la autorización del Responsable Funcional de los datos.

Deberá siempre hacerse uso de las **bases de datos centralizadas que contienen las direcciones e-mail y/o postales**, cuyos datos se encuentran actualizados y donde se han suprimido los datos de los destinatarios que así lo hayan solicitado.

Por el mismo motivo, **no está permitido guardar copias de las listas de direcciones de correo electrónico u hojas de etiquetas para envíos postales posteriores**, pues puede haber bajas o actualizaciones de datos antes del siguiente uso.

Los envíos masivos deben realizarse siempre con las aplicaciones específicas destinadas para ello (las instancias Sympa, Grupos de Google o Mailchimp de la Universidad[2]), que permiten gestionar de forma automatizada el consentimiento y las bajas y rectificación de datos de los interesados.

Sólo pueden realizarse envíos a quienes hayan dado previamente su consentimiento para ello; las Personas Trabajadoras deberán ser especialmente cuidadosas para evitar que los destinatarios de los correos electrónicos reciban publicidad o solicitudes de donación cuando no hayan solicitado información sobre las actividades y servicios de la Universidad o sobre como colaborar con el sostenimiento de la Universidad, sus actividades o el desarrollo de sus fines propios.

Queda prohibido cargar en las bases de datos direcciones electrónicas o postales que no se obtengan **directamente de sus titulares, prestando éstos su consentimiento**. En particular, está especialmente prohibido cargar direcciones en las bases a las que se haya accedido a través de redes sociales o cualquier método análogo.

El consentimiento de los titulares de las cuentas de correo electrónico **debe ser archivado** para atender posibles reclamaciones o ejercicio de derechos. **Supone una grave infracción de la ley dar de alta a otras personas en bases de datos de envíos sin su consentimiento, aunque se piense que puedan estar interesados en recibir la información u otra persona así lo haya asegurado.**

Todos los envíos tienen que adjuntar, obligatoriamente, una cláusula de información que incluya el Responsable del Tratamiento (generalmente será la Universidad o entidad que corresponda), la finalidad del envío, la causa jurídica que los legitima, la existencia de los derechos de acceso, rectificación, supresión y oposición y la forma de ejercerlos, así como la opción para darse de baja de envíos. Consulte la cláusula que debe utilizar al Delegado de Protección de Datos (dpo@unav.es).

Todos los formularios de recogida de datos tienen que adjuntar obligatoriamente una cláusula donde se informe al afectado de la finalidad de la recogida, de los destinatarios de los datos recogidos y de los datos necesarios para que el afectado pueda ejercer sus derechos. Consulte la cláusula que debe utilizar al Delegado de Protección de Datos.

[2] Consultar a IT Services o a la dirección dpo@unav.es para obtener más información sobre dichas herramientas y las condiciones de uso y acceso a las listas de destinatarios.

Los datos de carácter personal no podrán ser utilizados para finalidades distintas de aquellas para las que fueron recabados.

En los envíos de correos electrónicos dirigidos a varias personas, se incluirá la dirección de e-email propia como destinatario visible, y el resto de **destinatarios irán en el campo de copia oculta (CCO).**

8.9. ACCESO REMOTO

Todas las medidas precedentes también serán de aplicación cuando el acceso se produzca en la modalidad de acceso remoto desde fuera de los locales de la Universidad. El acceso remoto a los recursos debe realizarse siempre mediante VPN o HTTPS o los mecanismos de cifrado análogos que IT Services ponga a disposición de las Personas Trabajadoras.

9. NOTIFICACIÓN DE INCIDENCIAS DE SEGURIDAD INFORMÁTICA

Todo Empleado tiene obligación grave de comunicar cualquier incidencia o anomalía que afecte o se considere que puede afectar a la seguridad de los datos o de las comunicaciones[3], tanto en soporte informático como en soporte papel, al Responsable Funcional de los Datos, así como al Delegado de Protección de Datos y, en su caso, a IT Services. Su conocimiento y no comunicación puede ser considerada una negligencia grave a efectos disciplinarios.

10. POLITICAS DE DESCONEXION DIGITAL DE LAS PERSONAS TRABAJADORAS

Derecho a la desconexión digital en el ámbito laboral: Tal y como establece el artículo 88 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, las Personas Trabajadoras tienen derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

Periodos de desconexión: Se respetarán y garantizarán los tiempos de descanso de las Personas Trabajadoras, sus permisos y vacaciones, de acuerdo con la regulación del período de desconexión prevista en el Convenio Colectivo que resulte de aplicación para regular las relaciones laborales de las Personas Trabajadoras. En dichos periodos, con carácter general, no se contactará con las Personas Trabajadoras.

Excepciones: Sin perjuicio de las excepciones contempladas en el Convenio Colectivo, se podrá contactar con el personal fuera de su horario laboral para supuestos excepcionales y de carácter urgente, que puedan resolverse mediante una llamada o mensaje corto, salvo otros supuestos en los que se requiera de forma inmediata la intervención de la Persona Trabajadora para evitar un perjuicio para la Universidad.

Teletrabajo y desconexión: La Universidad garantizará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia dando cumplimiento a las normas legales o convencionales que resulten de aplicación a este respecto.

[3] Se incluyen todas aquellas incidencias que puedan afectar a la confidencialidad, la integridad y la disponibilidad de los datos, como por ejemplo: fallos del sistema que posibiliten el acceso a terceros no autorizados, pérdida o robo de información, sea en dispositivos móviles, dispositivos extraíbles como DVD o USB, formato papel, etc., pérdida o usurpación de contraseñas, elementos del Sistema de Información sin protección, etc.

11. CONSECUENCIAS DEL INCUMPLIMIENTO DE ESTA POLÍTICA

Cuando existan indicios suficientes o cuando se haya demostrado el incumplimiento real y efectivo de alguna de las estipulaciones contenidas en la Política, la Universidad de Navarra estará legitimada para realizar alguna o varias de las acciones que se enuncian a continuación, o cualquier otra que se considere oportuna, justificada y ajustada a la legislación vigente, con el objetivo último de garantizar el cumplimiento de la Ley, de la presente Política y, en su caso, de la normativa interna de desarrollo de la misma:

a. Solicitar a la Persona Trabajadora el cese de la actividad a través de la cual se haya producido el incumplimiento de la presente Política.
b. Bloquear el acceso, interrumpir la conexión y recuperar los dispositivos, equipos y demás medios tecnológicos que se hubieran utilizado o se estuvieran utilizando por la Persona Trabajadora para el desarrollo de la prestación de sus servicios.
c. Adoptar las medidas disciplinarias que, de conformidad con la legislación, Convenio Colectivo de aplicación o sus competencias, pudieran corresponderle, incluyendo, en los casos graves y culpables, la extinción de la relación laboral por despido disciplinario de la Persona Trabajadora, que se hará con arreglo al procedimiento legal y convencionalmente previsto, sin perjuicio de la reclamación de daños y perjuicios que pudieran derivarse del incumplimiento.
d. Iniciar las acciones legales que considere oportunas, de conformidad con la legislación nacional y europea vigente.

El conocimiento, observancia y respeto de la presente Política es vinculante para todos las Personas Trabajadoras de la Universidad cuando de forma directa o indirecta, accedan o hagan uso del Sistema de Información de la Universidad de Navarra.

12. MISCELÁNEA

La presente Política se aplicará a partir de su publicación en la Intranet de la Universidad. Sin perjuicio de lo anterior, la Universidad realizará un envío telemático a cada Persona Trabajadora para recabar su acuse de recibo en forma física o digital; la falta de firma o el desconocimiento de la normativa no eximirá al personal de su cumplimiento.

Sin perjuicio de lo anterior, IT Services podrá bloquear el acceso al Sistema de Información de la Universidad y a las herramientas tecnológicas (dispositivos móviles, portátiles, etc.) que la Universidad facilita a las Personas Trabajadoras.

Las Personas Trabajadoras de nueva incorporación deberán acusar recibo expresamente con carácter previo al inicio de su relación laboral en la primera sesión a la que accedan al Sistema de Información de la Universidad de Navarra; IT Services establecerá los mecanismos oportunos para garantizar esta obligación.

En caso de que exista contradicción entre otras políticas, procedimientos o disposiciones de la Universidad y la presente Política, ésta última prevalecerá en la medida de lo posible y en relación con su ámbito de ampliación.

La presente Política será examinada y revisada por el Comité de Seguridad y Privacidad siempre que se produzcan cambios significativos

- en la estructura organizativa de la Universidad o de IT Services,

- en el marco normativo o en los procesos o tecnologías empleados,
- después de un incidente de seguridad importante, si se produjese,
- cuando así lo recomiende una auditoría,
- cuando se produzca algún cambio en la normativa nacional o europea que exija una adaptación.
- y como mínimo, una vez cada dos años.

Las modificaciones y ajustes que pueda sufrir este documento, así como las nuevas versiones de la presente Política, se comunicarán a las Personas Trabajadoras a través de la Intranet y se comunicará la nueva versión al personal mediante correo electrónico, no siendo necesario recabar una nueva firma de las Personas Trabajadoras. Será obligación de las Personas Trabajadoras consultar la Intranet de la Universidad para conocer última versión disponible.

Devolución de documentación. Finalizada la relación laboral, acuerdo o convenio, o en cualquier momento, a solicitud de la entidad, el Trabajador o Trabajadora devolverá cualquier documentación, material o antecedente sustentado en cualquier tipo de soporte que constituya una información confidencial previamente facultada por cualquiera de las partes.

Cláusula de salvaguarda. Todas las cláusulas o extremos de este documento de uso deben ser interpretadas de forma independiente y autónoma, no viéndose afectadas el resto de estipulaciones en caso de que una de ellas haya sido declarada nula por sentencia judicial o resolución arbitral firme. Se sustituirá la cláusula o cláusulas afectadas por otra u otras que preserven los efectos perseguidos por las condiciones de uso.

Lista de distribución: Personas Trabajadoras de la Universidad de Navarra

13. CLAUSULAS INFORMATIVAS DE LOS PRINCIPALES TRATAMIENTOS DE PROTECCIÓN DE DATOS QUE AFECTAN A LOS TRABAJADORES

La Universidad de Navarra trata los datos personales de sus Trabajadores con diversas finalidades. A continuación, se recoge la cláusula informativa que corresponde a los tratamientos más importantes. Pueden consultarse las cláusulas de otros tratamientos en la información que los acompaña o solicitándolas al Delegado de Protección de Datos (dpo@unav.es).

Las Personas Trabajadoras se hacen responsables de la veracidad y de la actualización de la información y de los datos personales y familiares que suministren a la Universidad de Navarra para su tratamiento, quedando ésta exonerada de cualquier responsabilidad por su inexactitud, omisión o ausencia.

13.1. GESTIÓN DE LA RELACIÓN LABORAL

RESPONSABLE: Universidad de Navarra (R-3168001J), Campus Universitario, S/N, Edificio Central. 31080 Pamplona (Navarra, España).

FINALIDADES: Gestión de la relación laboral con el Trabajador o Trabajadora y pago de nóminas. Prevención de riesgos laborales. Formación. Evaluación, seguimiento y control del desarrollo de las actividades

profesionales. Captación de su imagen en fotografía y/o video para su publicación en el directorio de Trabajadores, así como en la página web y redes sociales u otros medios de comunicación para promocionar los servicios y actividades de la Universidad y mantener el archivo histórico de imágenes y sonidos. Envío de comunicaciones internas de información general de la Universidad, eventos, necesidades, felicitaciones de cortesía y actos organizados.

LEGITIMACIÓN: Obligación legal por parte del Responsable del Tratamiento de cumplir, entre otras normas legales: Convenio Colectivo, Estatuto de los Trabajadores, Ley General Tributaria, Ley del Impuesto de la Renta de las Personas Físicas (Estatal y Foral de Navarra), Decreto Foral de la Diputación Foral de Guipúzcoa sobre el Impuesto de la Renta de las Personas Físicas; Ley de Mutuas de Accidentes de Trabajo y Enfermedad Profesional; Ley de Enjuiciamiento Civil; Código Penal; Fuero Nuevo de Navarra; Código Civil; Ley de Prevención de Riesgos Laborales. Interés legítimo del Responsable del Tratamiento en mantener un archivo histórico de imágenes así como promocionar sus servicios y actividades. Ejecución de contrato laboral.

CESIONES: Entre los centros de la Universidad por motivos de organización y gestión de las actividades. Administraciones Públicas y entidades bancarias para la gestión laboral y el pago de nóminas. Mutuas laborales, compañías de seguros y empresas de prevención de riesgos laborales. Despachos de Abogados; Auditores y empresas dedicadas a la Consultoría que prestasen servicios a la Universidad para mejor cumplimiento de sus finalidades. Aquellas entidades, clientes y proveedores ante las cuales sea necesario identificar a las Personas Trabajadoras. Empresas de formación y tramitación de bonificaciones ante la Fundación Estatal para el Empleo. Servicios auxiliares.

CONSERVACIÓN: Serán conservados durante la vigencia del contrato laboral y, finalizada ésta, se conservarán bloqueados durante los plazos exigidos legalmente para atender eventuales responsabilidades, con carácter general 4 años. La Universidad conservará, con carácter indefinido, en base a un interés legítimo en mantener un registro histórico de Trabajadores, los datos identificativos, historial del puesto de trabajo y curriculum, así como las imágenes y registros de audio y vídeo en el archivo histórico de la Universidad.

DERECHOS: Toda Persona Trabajadora tiene derecho a solicitar, mediante un escrito dirigido al Delegado de Protección de Datos (dpo@unav.es), el acceso, rectificación, supresión, oposición, limitación y portabilidad de sus datos. En caso de que considere vulnerados sus derechos en relación con el tratamiento de sus datos personales, puede presentar una reclamación ante la Agencia Española de Protección de Datos (www.agpd.es).

NOTA: En ocasiones, la Universidad pone a disposición de las Personas Trabajadoras el acceso al repertorio fotográfico o en vídeo de algunos eventos privados y familiares en los que participan. El uso de las imágenes debe ceñirse exclusivamente **al ámbito privado y familiar**, por lo que no se puede hacer uso de las mismas para su publicación en otros medios, por ejemplo, en redes sociales, sin contar con el consentimiento de cada uno de los participantes en las imágenes.

13.2. VIDEOVIGILANCIA

RESPONSABLE: Universidad de Navarra (R-3168001J), Campus Universitario, S/N, Edificio Central. 31080 Pamplona (Navarra, España).

FINALIDADES: Preservar la seguridad de las personas, bienes e instalaciones en el Campus y, en su caso y de acuerdo con la Legislación vigente, denunciar, cuando sea necesario, hechos ante las autoridades competentes o atender los requerimientos de las mismas, o reclamar ante las Entidades Aseguradoras.

LEGITIMACIÓN: Las bases que legitiman el tratamiento son: el interés legítimo en garantizar la seguridad e integridad de estas instalaciones por parte de su titular, lo que justifica que los datos sean captados necesariamente por el hecho de acceder a este recinto; las obligaciones legales del Responsable del Tratamiento. Asimismo el consentimiento de los titulares de vehículo que deseen estacionar en los lugares reservados por la Universidad para ello.

CESIONES: Administraciones Públicas y entidades judiciales y autoridades si lo solicitasen y procediese su cesión. Entidades Aseguradoras. Otros usuarios de los lugares habilitados como estacionamiento por la Universidad de Navarra que pudiesen verse afectados por incidentes o daños en sus vehículos.

CONSERVACIÓN: Los datos serán conservados durante un periodo máximo de un mes, salvo que fuese necesario conservarlos durante más tiempo para esclarecer alguna infracción u otro hecho detectado en relación con las finalidades del tratamiento.

DERECHOS: Toda Persona Trabajadora tiene derecho a solicitar el acceso, rectificación, supresión, oposición, limitación y portabilidad de sus datos, mediante un escrito dirigido al Delegado de Protección de Datos (dpo@unav.es). En caso de que considere vulnerados sus derechos en relación con el tratamiento de sus datos personales, puede presentar una reclamación ante la Agencia Española de Protección de Datos (www.agpd.es).

13.3. CONTROL DE ACCESOS Y REGISTRO DE JORNADA

RESPONSABLE: Universidad de Navarra (R-3168001J), Campus Universitario, S/N, Edificio Central. 31080 Pamplona (Navarra, España).

FINALIDADES:

- Mantener un registro de jornada con carácter individual de cada Trabajador y Trabajadora.
- Preservar la seguridad de las personas, bienes e instalaciones.

LEGITIMACIÓN: Dar cumplimiento a la obligación legal del Responsable del Tratamiento de mantener un registro de jornada con carácter individual de cada Trabajador o Trabajadora (Art. 34.9 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores); interés legítimo en garantizar la seguridad e integridad de las persona, bienes e instalaciones.

CESIONES: Administraciones Públicas y entidades judiciales y autoridades si lo solicitasen y procediese su cesión.

CONSERVACIÓN: Los datos serán conservados durante un periodo máximo de cuatro años.

DERECHOS: Toda Persona Trabajadora tiene derecho a solicitar el acceso, rectificación, supresión, oposición, limitación y portabilidad de sus datos, mediante un escrito dirigido al Delegado de Protección de Datos (dpo@unav.es). En caso de que considere vulnerados sus derechos en relación con el tratamiento de sus datos personales, puede presentar una reclamación ante la Agencia Española de Protección de Datos (www.agpd.es).

13.4. REGISTRO DE ACCESOS A INTERNET

RESPONSABLE: Universidad de Navarra (R-3168001J), Campus Universitario, S/N, Edificio Central. 31080 Pamplona (Navarra, España).

FINALIDADES: Gestión del funcionamiento y rendimiento de las redes internas y de la conexión a Internet. Gestión del cumplimiento de las leyes, políticas y reglamentos que sean de aplicación. Gestión de incidentes de seguridad. Velar por el cumplimiento de esta política.

LEGITIMACIÓN: Interés legítimo de la Universidad de Navarra en gestionar dichas finalidades. Obligación legal del Responsable del Tratamiento.

CESIONES: A la autoridad judicial, en los casos en que sean legalmente exigibles.

CONSERVACIÓN: 1 año.

DERECHOS: El interesado tiene derecho a solicitar el acceso, rectificación, supresión, oposición, limitación y portabilidad de sus datos, mediante un escrito dirigido al Delegado de Protección de Datos (dpo@unav.es). En caso de que considere vulnerados sus derechos en relación con el tratamiento de sus datos personales, puede presentar una reclamación ante la Agencia Española de Protección de Datos (www.agpd.es).

13.5. GESTIÓN Y DIFUSIÓN DE LA INVESTIGACIÓN

RESPONSABLE: Universidad de Navarra (R-3168001J), Campus Universitario, S/N, Edificio Central. 31080 Pamplona (Navarra, España).

FINALIDADES Y BASES DE LEGITIMACIÓN:

i. Gestión de actividades y proyectos de investigación en sus distintas fases (propuesta, en curso, realizada, etc.) que se realizará en virtud de la necesaria ejecución de la relación laboral existente entre las partes.

ii. Gestión y publicación por medios físicos o electrónicos, incluida Internet, de currícula del personal docente e investigador que se realizará en virtud de la necesaria ejecución de la relación laboral existente entre las partes.

iii. Difusión de la investigación por medios físicos o electrónicos, incluida su publicación en Internet que se realizará en virtud del interés legítimo del Responsable del Tratamiento en dar visibilidad a la actividad investigadora.

OBTENCIÓN DE LOS DATOS: Del propio interesado y/o de repositorios públicos de investigación.

CESIONES: A la autoridad judicial, en los casos en que sea legalmente exigible. En el marco de los convenios y acuerdos de investigación que pudieran concertarse con terceros, se podrían producir cesiones a éstos.

TRANSFERENCIAS INTERNACIONALES: En el marco de los convenios y acuerdos de investigación que pudieran concertarse con terceros, se podrían producir transferencias internacionales de datos personales, con las garantías que dispone el Reglamento Europeo de Protección de Datos.

PLAZO DE CONSERVACIÓN: Con carácter general, los datos personales se conservarán mientras dure la relación entre el interesado y la Universidad de Navarra y, posteriormente, mientras sea necesario para el cumplimiento de las finalidades indicadas o, en su caso, debidamente bloqueados mientras sean exigibles responsabilidades legales.

DERECHOS: El interesado tiene derecho a solicitar el acceso, rectificación, supresión, oposición, limitación y portabilidad de sus datos, mediante un escrito dirigido al Delegado de Protección de Datos (dpo@unav.es). En caso de que considere vulnerados sus derechos en relación con el tratamiento de sus datos personales, puede presentar una reclamación ante la Agencia Española de Protección de Datos (www.aepd.es).

14. MAPA DE CLÁUSULAS Y CONTROLES ISO 27001:2015 E ISO 27701:2019

A.6 Organización de la seguridad de la información

A.6.2 Dispositivos móviles y teletrabajo

Objetivo: Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles

ISO 27001 Control A.6.2.1	Política de dispositivos móviles	*Control* Se debería adoptar una política y unas medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles	ISO 27701 Control 6.5.1.3	La organización debe asegurarse que el uso dispositivos móviles no afecta a la protección de datos personales.
ISO 27001 Control A.6.2.2	Teletrabajo	*Control* Se debería adoptar una política y unas medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo	ISO 27701 Control 6.5.1.4	Sin cambios.

A.8 Gestión de Activos

A.8.1 Responsabilidad sobre los activos

Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección de datos.

ISO 27001 Control A.8.1.3	Uso aceptable de los activos	*Control* Se deberían identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información	ISO 27701 Control 6.5.1.3	Sin cambios.
ISO 27001 Control A.8.1.4	Devolución de activos	*Control* Todas las Personas Trabajadoras y terceras partes deberían devolver todos los activos de la organización que estén en su	ISO 27701 Control 6.5.1.4	Sin cambios.

		poder al finalizar su empleo, contrato o acuerdo.		

A.11 Seguridad física y del entorno

A.11.2 Seguridad de los equipos

Objetivo: Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización

ISO 27001 Control A11.2.8	Equipo de usuario desatendido	*Control* Los usuarios deberían asegurarse de que el equipo desatendido tiene la protección adecuada	ISO 27701 Control 6.8.3.8	Sin cambios.
ISO 27001 Control A.11.2.9	Política de puesto despejado y pantalla limpia	*Control* Debería adoptarse una política de puesto de trabajo despejado de papeles y medios de almacenamiento desmontables y política de pantalla limpia para los recursos de tratamiento de la información	ISO 27701 Control 6.8.3.9	La organización debe limitar el uso de copias impresas de información de carácter personal al mínimo imprescindible para la operación

A.12 Seguridad de las operaciones

A.12.5 Control del software en explotación

Objetivo: Asegurar la integridad del software en explotación

ISO 27001 Control A12.6.2	Restricción en la instalación de software	*Control* Se deberían establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios	ISO 27701 Control 6.9.6.2	Sin cambios.

A.13 Seguridad de las comunicaciones

A.13.2 Intercambio de información

Objetivo: Mantener la seguridad en la información que se transfiere dentro de una organización y con cualquier entidad externa

ISO 27001 Control A13.2.1	Políticas y procedimientos de intercambio de información	*Control* Deberían establecerse políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso de todo tipo de recursos de comunicación	ISO 27701 Control 6.10.2.1	La organización debe establecer procedimientos para asegurar que las normas vinculadas al procesamiento de datos de carácter personal se aplican tanto dentro como fuera del sistema cuando sea necesario

15. CONTROL DE VERSIONES

CONTROL DE VERSIONES						
Versión		Resumen modificaciones	Elaborado	Revisado	Revisado	Aprobado
Nº	Fecha					
14	06/11/2017	Se consolida una nueva versión conforme al RGPD	DPO	Asesoría Jurídica	Responsable de Seguridad de la Información	
14.1	08/05/2018	Se modifican las políticas de passwords	IT Services	IT Services	Responsable de Seguridad de la Información	DPO
14.2	24/05/2018	Se corrige una errata en la pág 8	Responsable de Seguridad de la Información			
14.3	09/11/2018	Se modifican las características de la fortaleza de la contraseña para adecuarlas al nuevo procedimiento de Accouting aprobado en octubre de 2018 Se elimina un párrafo repetido en la p 8	Responsable de Seguridad de la Información			
14.4	16/12/2018	Se modifica la política de fortaleza de contraseñas	Responsable de Seguridad de la Información			
15a	26/01/2021	Nueva versión adecuada a las normas ISO 27001 - ISO 27701	IT Compliance & Data Governance			
15f	01/04/2022	Consolidación de la nueva versión	IT Compliance DPO	Asesoría Jurídica Externa	IT Services Asesoría Jurídica	Comisión de Seguridad y Privacidad
15g	01/04/2022	Corrección de erratas	IT Compliance DPO			
15g2	13/05/2022	Cambios en la redacción de algunos apartados y adición de notas para facilitar la comprensión; corrección de errores	IT Compliance DPO	Asesoría Jurídica		Comisión de Seguridad y Privacidad

Recibido y leído el presente documento: