Universidad de Navarra

POLÍTICA DE FUNCIONES Y OBLIGACIONES DE LOS USUARIOS EN MATERIA DE SEGURIDAD Y PROTECCIÓN DE DATOS

UNIVERSIDAD DE NAVARRA

CIF: R3168001J

Campus Universitario, S/N. Edificio Central. 31080, Pamplona

CONTROL DE VERSIONES						
Versión		Resumen modificaciones	Elaborado	Revisado	Aprobado	Aprobado
Nº	Fecha					
14	06/11/2017	Se consolida una nueva versión	Asesoría Jurídica	IT Services	Responsable de Seguridad	Responsable de Fichero
14.1	08/05/2018	Se modifican las políticas de passwords	IT Services	IT Services	Responsable de Seguridad	DPO
14.2	24/05/2018	Se corrige una errata en la pág 8	Responsable de Seguridad			DPO
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			DPO
14.4	15/06/2021	Se corrigen algunas erratas	Responsable Data Governance			DPO

INDICE

1. OBJETO Y ÁMBITO DE APLICACIÓN

El objeto de la presente política es regular aspectos básicos de seguridad de la información y protección de datos.

En particular, esta política presta especial atención al uso que se realiza de las siguientes **herramientas de trabajo**:

- Internet.
- Cuentas de correo corporativas.
- Equipos informáticos y dispositivos extraíbles.

La política resulta de aplicación a todos los **trabajadores** y **colaboradores** de la **UNIVERSIDAD DE NAVARRA** (en adelante, "**UNAV**" o la "**Universidad**") a los que se les haya facilitado acceso a las instalaciones, sistemas y/o herramientas de trabajo propiedad de dicha organización para el desarrollo de sus funciones (en adelante, nos referiremos a los trabajadores y colaboradores conjuntamente como "**usuarios**").

2. USO DEL CORREO ELECTRÓNICO CORPORATIVO

2.1. NORMAS GENERALES

UNAV proporciona a los empleados y colaboradores una cuenta de correo corporativo, cuya dirección está formada por la inicial del nombre y el apellido completo del usuario (o una combinación similar), seguidos de "@unav.es", "@unav.edu" y/o "@tecnun.es".

La cuenta de correo es una herramienta de comunicación que UNAV pone a disposición de los usuarios **para fines relacionados con la actividad de la Universidad.** Por tanto, **no está permitido el uso personal del correo electrónico corporativo**.

No obstante, se tolerará un uso limitado para fines particulares siempre que no atente contra la imagen de la Universidad, no interfiera en su actividad y no afecte a la productividad del usuario.

En todo caso, se encuentran prohibidas las siguientes prácticas:

- **Utilización de la cuenta corporativa para el desarrollo de actividades profesionales o comerciales privadas.**
- **Difusión de contenidos contrarios a las leyes o que vulneren los derechos de terceros.** Por ejemplo, y a título meramente enunciativo, (i) la difusión de materiales que vulneren derechos de propiedad intelectual o industrial de terceros, (ii) la difusión de contenidos violentos o amenazas, o (iii) la difusión de mensajes xenófobos, racistas o que realicen apología del terrorismo.
- **Falsificación de cabeceras**. Todas las comunicaciones realizadas a través del correo electrónico deben estar plenamente identificadas con la información de contacto del remitente. En este sentido, se prohíbe falsear, disimular, suprimir o reemplazar la identidad de un usuario, así como realizar cualquier actividad que tenga la intención de encubrir la identidad del usuario.

- **Distribución de correos electrónicos no solicitados ("spam") o e-mails en cadena.**
- **Cualquier otra actividad que contravenga las disposiciones legales vigentes.**

2.2. ACCESO AL CORREO ELECTRÓNICO DEL USUARIO

UNAV podrá acceder al buzón de correo de los usuarios para realizar tareas de mantenimiento técnico o para continuar con su actividad diaria en caso de bajas temporales o definitivas, o periodos de vacaciones.

Dicho acceso se llevará a cabo por personal técnico. Los usuarios no deben facilitar sus contraseñas a terceros o a compañeros de trabajo bajo ninguna circunstancia.

Cuando un usuario se ausente por más de cinco días laborables de su puesto de trabajo, incluyendo bajas temporales y vacaciones, deberá colocar un aviso automático haciéndolo saber e indicando los datos de contacto de la persona que le sustituye.

En caso de baja definitiva del usuario, el personal técnico de UNAV activará dicho aviso automático indicando que la cuenta no se encuentra operativa.

Dado que, como se ha señalado, las cuentas de correo electrónico son herramientas de trabajo destinadas a un uso profesional, UNAV **no asumirá ninguna responsabilidad sobre la información personal contenida en los buzones de los usuarios**.

2.3. CONSERVACIÓN DE CORREOS ELECTRÓNICOS

Los usuarios conservarán aquellos correos electrónicos que contengan documentos de trabajo o comunicaciones con terceros de relevancia para la Universidad. Igualmente, deberán guardar y clasificar los archivos adjuntos a los correos electrónicos necesarios para el adecuado desarrollo de sus funciones.

2.4. FIRMA Y AVISO LEGAL EN LOS CORREOS

Es obligatorio que todos los usuarios utilicen la firma corporativa y el aviso de confidencialidad aprobado por la Universidad.

Los usuarios deberán identificarse en los correos salientes con una firma que siga el siguiente estándar:

Todos los correos electrónicos tendrán que incluir el siguiente aviso de confidencialidad después de la firma:

"Este mensaje puede contener información confidencial. Si usted no es el destinatario del mismo 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/colaboradores y terceros. Puede consultar la Política de Privacidad la Universidad de Navarra en la dirección: https://www.unav.edu/aviso-legal"

3. USO DE INTERNET

3.1. NORMA GENERAL

La Universidad pone a disposición de los usuarios un acceso a Internet **que sólo deberá utilizarse para fines profesionales** relacionados con las funciones que desempeñen dentro de UNAV.

No obstante lo anterior, **se tolerará una utilización personal** del acceso a Internet en la medida en que no afecte a la productividad del usuario ni a la seguridad de los sistemas de la Universidad.

3.2. CONTROL DEL ACCESO A INTERNET

Los usuarios quedan informados de que **por motivos técnicos y de seguridad** se realiza un control de los accesos a Internet efectuados. **Se recuerda a los usuarios que la navegación por algunas páginas y la descarga de programas/aplicaciones no autorizadas puede conllevar daños en los equipos y sistemas y/o contravenir la legislación vigente**.

La Universidad ha implementado **un sistema de seguridad en el acceso a Internet con las siguientes características**:

1) **Registro** de la actividad de cada usuario en Internet, que contiene los siguientes datos: usuario, máquina, dirección IP, páginas visitadas, fecha y hora, tiempo de conexión, ancho de banda, tipología de páginas visitadas, páginas bloqueadas, páginas

permitidas. Los registros se consultarán en caso de que se detecte alguna irregularidad.

2) **Bloqueo de navegación** por determinadas páginas en Internet, según la categorización establecida por IT Services. El sistema de seguridad mostrará un mensaje al usuario en el caso en que sea bloqueada alguna página.

3) **Estadísticas** de consumo de recursos, entendiéndose por recursos tanto el tiempo de conexión como el ancho de banda consumida.

4. EQUIPOS INFORMÁTICOS

4.1. NORMAS GENERALES

Los equipos informáticos asignados a los usuarios **son herramientas de trabajo**. En este sentido, el usuario queda informado expresamente de lo siguiente:

- **El personal técnico de UNAV puede acceder a los equipos informáticos, físicamente o en modo remoto, para realizar tareas de mantenimiento o reparación. UNAV no asume ninguna responsabilidad en caso de pérdida, deterioro, destrucción o acceso a documentos privados de los usuarios almacenados en los equipos informáticos**.
- Los equipos pueden ser reasignados a otros usuarios, según disponibilidad y necesidades de la Universidad.

Los usuarios 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 el usuario.**

Se recomienda realizar copias periódicas de la información contenida en los ordenadores en las carpetas de red o Google Drive de los usuarios.

Los usuarios deben trabajar utilizando las aplicaciones, programas y bases de datos centrales.

Está expresamente prohibido generar o almacenar en los equipos informáticos ficheros de datos personales o ficheros temporales de datos personales sin obtener una autorización previa siguiendo los procedimientos descritos en el *Documento de Seguridad.*

Los equipos han sido configurados por IT Services con los accesos y programas necesarios para que cada usuario realice su trabajo.

Los cambios en la configuración o la instalación de software adicional deberán ser solicitados a través de IT Services.

Salvo que el usuario haya obtenido una autorización para ello conforme a los procedimientos descritos en el *Documento de Seguridad* y en el presente documento, **no se podrán realizar copias de datos personales ni documentos confidenciales almacenados en sistemas de UNAV**

utilizando soportes extraíbles, sistemas personales de almacenamiento en la nube, etc. ni sacar dichos documentos fuera de las instalaciones de la UNAV.

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

El tratamiento de datos personales fuera de los locales de la Universidad requiere autorización previa. En este sentido, todos los usuarios que, en base a su perfil profesional, cuenten con un equipo portátil u otro tipo de dispositivo móvil proporcionado por UNAV (en adelante, los "**Dispositivos**") dispondrán de dicha autorización.

No está permitido el tratamiento de datos personales en Dispositivos que no sean propiedad de la Universidad.

El usuario debe firmar un documento en el momento de la entrega del Dispositivo para que quede constancia de la misma, haciéndose responsable de la seguridad y custodia de los datos de carácter personal que puedan quedar almacenados de forma local en él (Formulario del ANEXO 8.1 del *Documento de Seguridad*).

Los Dispositivos asignados son herramientas de trabajo **para uso personal e intransferible del usuario**. No podrán ser compartidos con terceros (compañeros de trabajo, familiares, etc.).

La pérdida o robo de un Dispositivo debe ser inmediatamente notificado al Centro de Atención al Usuario (CAU) de IT Services y al Delegado de Protección de Datos *(Data Protection Officer)* de la Universidad (dpo@unav.es).

Los usuarios pueden dirigirse a IT Services para recibir información sobre mecanismos de cifrado de la información contenida en los Dispositivos.

5. DISPOSITIVOS EXTRAÍBLES

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

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

Sólo está permitido el uso de Dispositivos Extraíbles propiedad del usuario para almacenar documentos de trabajo que no estén clasificados como confidenciales (por ejemplo, los profesores e investigadores pueden utilizar dispositivos propios para conservar artículos, tesis, publicaciones, material de las clases, etc.).

Como norma general, los usuarios no deben utilizar Dispositivos Extraíbles (ni propios ni facilitados por la UNAV) para almacenar datos de carácter personal y/o información confidencial.

Se recuerda que está prohibido generar ficheros temporales que contengan datos personales, en particular las que contengan datos personales de los alumnos de la Universidad.

En el caso de que sea **estrictamente necesario** almacenar datos de carácter personal en Dispositivos Extraíbles, se actuará conforme a los procedimientos indicados en el *Documento de Seguridad.*

Cuando se trate de información confidencial que no contenga datos personales se deberá:

- Solicitar la autorización del responsable de dicha información.
- Pedir asesoramiento a IT Services sobre mecanismos de cifrado.
- Utilizar el Dispositivo Extraíble exclusivamente para almacenar la información confidencial, sin mezclarla con otra información no confidencial o personal.
- Etiquetar el Dispositivo para reducir el riesgo de pérdida.
- Borrar el contenido del Dispositivo una vez haya dejado de ser necesaria la información que contiene.

La pérdida o robo de un Dispositivo Extraíble que contenga datos de carácter personal o información confidencial debe ser inmediatamente notificada al Centro de Atención al Usuario (CAU) de 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. Los usuarios que deseen desechar un Dispositivo Extraíble, deberán notificarlo a la siguiente Centro de Atención al Usuario (CAU).

6. ALMACENAMIENTO EN LA NUBE

No está permitido a los usuarios el almacenamiento de datos personales en la nube *(cloud).*

El resto de información relacionada con las actividades de UNAV solamente podrá almacenarse en los servicios *cloud* que se encuentren bajo los acuerdos suscritos por la Universidad con Google y Microsoft para la utilización de las plataformas Google Apps y Microsoft Online respectivamente.

No podrán utilizarse servicios públicos de almacenamiento en la nube distintos de los citados en el párrafo anterior, por desconocerse las condiciones de integridad, disponibilidad y confidencialidad de la información del proveedor del servicio, así como las garantías de salvaguarda de la propiedad intelectual, si fuera el caso.

7. GESTIÓN DE CONTRASEÑAS

Para desarrollar las tareas diarias, se ha asignado a cada usuario unas claves de acceso (un nombre de usuario y una contraseña) que deberá introducir para acceder a su equipo informático y a la mayoría de las aplicaciones.

Adicionalmente, es posible que se asignen claves de acceso específicas a los usuarios de algunas aplicaciones concretas.

Las contraseñas deberán cumplir los siguientes requisitos *[en cursiva modificaciones del 9/11/2018]:*

1. Estar formadas por al menos 10 caracteres *y 64 como máximo*.
2. *La contraseña es más segura cuantos más caracteres tenga, siendo una buena práctica utilizar frases de contraseñas o passphrase.*
3. *Estar formada por letras (salvo ñ) mayúsculas y minúsculas, y números. Se recomienda incluir al menos un carácter especial del tipo ./+-|":$%*3.*
4. La contraseña caducará a los 12 meses y no se podrá repetir en las próximas *5* rotaciones.

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 del usuario o a la persona que le sustituya durante periodos de baja).

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

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

8. POLÍTICA DE MESAS LIMPIAS Y GESTIÓN DE DOCUMENTACIÓN EN SOPORTE PAPEL

8.1. NORMA GENERAL

Cada usuario es responsable de la adecuada custodia de la documentación en soporte papel que genera y/o utiliza para el desarrollo de sus tareas.

Los distintos departamentos o áreas de la Universidad fijarán criterios de archivo, en función de sus necesidades, que permitan mantener la información en soporte papel organizada de forma lógica y faciliten la búsqueda de documentos.

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

La documentación confidencial y/o que mantenga datos de carácter personal debe ser almacenada en armarios, archivadores o dependencias que dispongan de un sistema de cerrado con llave o mecanismo equivalente (por ejemplo, tarjeta electrónica, código, etc.). El responsable del archivo será el encargado de custodiar la llave o mecanismo de acceso.

A título meramente enunciativo, se señalan los siguientes ejemplos de documentos que deben almacenarse en lugares cerrados:

- Expedientes académicos de alumnos.
- Documentación que contenga comentarios y valoraciones de tutores en relación a los alumnos.
- Información relativa a recaudación de fondos.
- Información relativa a donantes.
- Información relativa al personal de la Universidad (situaciones de baja, solicitud de permisos, nóminas, etc.).

En ningún caso, deberán ubicarse archivos en zonas de paso (por ejemplo, pasillos, recepciones, etc.), aunque se almacenen en estanterías o armarios cerrados. En caso de no disponer de los archivadores, cajoneras, armarios, etc. necesarios para el adecuado archivo de los documentos confidenciales, el usuario debe solicitarlos al Servicio de Compras.

8.2. POLÍTICA DE MESAS LIMPIAS

Al finalizar la jornada laboral, los usuarios dejarán su escritorio despejado, archivando los documentos con los que han estado trabajando durante la jornada ("Política de Mesas Limpias").

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.

Está prohibido depositar en papeleras de oficinas o contenedores documentos que contengan datos de carácter personal y/o información confidencial (expedientes de alumnos o trabajadores, listados de calificaciones, fichas de alumnos, etc.).

9. ENVÍOS MASIVOS POR CORREO ELECTRÓNICO U ORDINARIO

No está permitido que los usuarios realicen envíos masivos por correo electrónico u ordinario sin la autorización del responsable de su centro o servicio.

Deberá siempre hacerse uso de las **listas de direcciones e-mail o postales centralizadas**, que tienen actualizados los posibles repudios ejercidos por los destinatarios de los envíos.

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 repudios antes del siguiente uso.

Los envíos masivos deben realizarse siempre con copia oculta.

10. DEBER DE SECRETO

Los usuarios que acceden a datos de carácter personal o información confidencial están obligados a guardar secreto en relación a los mismos, sea cual sea su función en la Universidad y el cargo que ocupen.

Los usuarios deben evitar prácticas como:

- Comentar con terceros expedientes de alumnos y calificaciones. Sólo los propios alumnos y, en determinadas circunstancias 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 intercambiar listados de alumnos/calificaciones a través de la aplicación "*WhatsApp*".
- Discutir asuntos confidenciales en espacios públicos (cafeterías, pasillos, etc.).

11. NOTIFICACIÓN DE INCIDENCIAS

Cualquier incidencia relativa a seguridad o protección de datos debe ser comunicada de forma inmediata al Centro de Atención al Usuario (CAU) de IT Services y al Delegado de Protección de Datos *(Data Protection Officer)* de la Universidad (dpo@unav.es).

12. CONSECUENCIAS DEL INCUMPLIMIENTO

El incumplimiento de las medidas de seguridad recogidas en este documento se considerará una infracción grave, que podrá dar lugar a la apertura de un procedimiento disciplinario frente al usuario incumplidor.