



# Universidad de Valladolid

## NORMAS DE USO DEL CORREO ELECTRÓNICO (Aprobadas por el Consejo de Gobierno en sesión de 27 de mayo de 2020)

### ÍNDICE

1. Objeto.....	2
2. Alcance .....	2
3. Vigencia .....	2
4. Revisión y evaluación .....	2
5. Custodia y difusión.....	3
6. Garantía de los derechos de los usuarios.....	3
7. Normativa .....	4
8. Testamento digital .....	11



## Universidad de Valladolid

### 1. Objeto

La Universidad de Valladolid pone a disposición de los miembros de la comunidad universitaria distintos recursos ordenados al tratamiento de información. Entre ellos, el servicio de correo electrónico (e-mail), que permite la remisión de información valiosa para la institución, sea esta personal o no, y define un ámbito de comunicaciones constitucionalmente relevante.

El [Reglamento de notificaciones y comunicaciones electrónicas en la Universidad de Valladolid](#) (aprobado por el Consejo de Gobierno en sesión de 28 de junio de 2019) regula en su título III el uso de las comunicaciones electrónicas y establece la obligatoriedad de utilización de medios electrónicos para las comunicaciones internas de los empleados públicos universitarios.

El correo electrónico es un servicio de red que posibilita enviar y recibir mensajes con ficheros adjuntos. Las características peculiares de este medio de comunicación, como la universalidad o su bajo coste, han propiciado la aparición de amenazas que aprovechan sus vulnerabilidades para propagarse.

El objetivo de la presente norma es regular el acceso y utilización del correo electrónico por parte de los usuarios de los sistemas de información de la Universidad de Valladolid, estableciendo las directrices generales que permitan garantizar la seguridad de la información y proteger los derechos de las personas. Para conseguirlo, se definen criterios y reglas de uso homogéneos para todos los usuarios del servicio de correo electrónico.

### 2. Alcance

La presente norma se aplica a todo el ámbito de actuación de la Universidad de Valladolid y sus contenidos derivan de las directrices de carácter general definidas en el documento de [Política de Seguridad de la Información](#).

Este documento resulta de aplicación y de obligado cumplimiento para todos los usuarios del servicio de correo electrónico, incluyendo aquellos usuarios de organizaciones externas que posean acceso al sistema de la Universidad de Valladolid.

### 3. Vigencia

La presente norma, consensuada previamente con los representantes de los trabajadores, ha sido propuesta por el Comité de Seguridad de la Universidad de Valladolid y aprobada por el Consejo de Gobierno el día 27 de mayo de 2020. Surtirá efectos al día siguiente de su publicación en el Tablón electrónico de anuncios de la sede electrónica de la UVa. La norma deroga cualesquiera recomendaciones previas.

### 4. Revisión y evaluación

La gestión de esta normativa corresponde al Comité de Seguridad de la Información que es competente para:



## Universidad de Valladolid

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

Anualmente, el Comité de Seguridad de la Información revisará la presente normativa. No obstante, el Comité podrá realizar revisiones en cualquier momento cuando considere que concurren circunstancias para ello.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general o cualquier otra circunstancia relevante.

### 5. Custodia y difusión

Corresponde al Responsable de Seguridad la custodia y divulgación de la versión aprobada de este documento.

### 6. Garantía de los derechos de los usuarios

El correo electrónico constituye una herramienta que el empleador pone a disposición de los trabajadores para el desarrollo de la actividad profesional y de los alumnos para la prestación del servicio público de educación superior.

Se garantiza el secreto de las comunicaciones. El personal técnico del servicio viene obligado a guardar un especial deber de secreto y confidencialidad.

En la prestación del servicio de correo electrónico la Universidad de Valladolid aplicará los siguientes criterios:

6.1. Únicamente se accederá al buzón de correo electrónico en virtud de mandato judicial. Si el acceso a los mensajes del buzón de correo electrónico fuese requerido, este se llevará a cabo con las máximas garantías, adoptando las medidas necesarias que permitan preservar la integridad, confidencialidad y trazabilidad de la información.

6.2. En los casos en que resulte de absoluta necesidad, se requerirá la autorización previa de las personas usuarias para acceder al buzón de la cuenta de correo electrónico. Se considera que concurre necesidad al menos en los siguientes casos:

- Cuando la cuenta se vincule a finalidades de gestión administrativa o académica y se prevea una ausencia prolongada del titular resultando necesario el acceso para recuperar información relevante para el funcionamiento del servicio.
- Cuando se constaten amenazas o violaciones de la seguridad que tengan origen en la cuenta.
- Cuando la incidencia reportada por el titular de la cuenta sólo pueda ser resuelta



## Universidad de Valladolid

mediante acceso a la misma.

6.3. Podrán realizarse acciones automatizadas para proteger el normal funcionamiento del servicio. Estas acciones tendrán como finalidad la detección o eliminación de *spam* y código malicioso.

6.4. Los titulares de las cuentas de correo electrónico están obligados a crear en su cuenta de correo electrónico de la Universidad de Valladolid una carpeta con la rúbrica “personal” en caso de que acogiéndose a lo dispuesto en la norma 7.7 realicen algún uso particular. Esta carpeta será preservada respecto de cualquier acceso, salvo autorización de la persona titular, y será tenida en cuenta en relación con las previsiones de esta normativa previstas en la sección sobre testamento digital.

6.5. Los titulares de cuentas de correo electrónico que con motivo del desarrollo de la actividad investigadora deban respetar derechos de propiedad intelectual, secreto industrial, patentes, marcas, obligación de secreto y confidencialidad u otros derechos equivalentes, incluirán esta información en una carpeta con la rúbrica “confidencial”. Esta carpeta será preservada respecto de cualquier acceso, salvo autorización de la persona titular, excepto que se trate de derechos titularidad de la Universidad de Valladolid, y será tenida en cuenta en relación con las previsiones de esta normativa previstas en la sección sobre testamento digital.

6.6. No existe expectativa de privacidad o secreto de las comunicaciones en las cuentas de naturaleza estrictamente institucional. Este tipo de cuentas son utilizadas normalmente para la prestación de algún servicio de manera genérica y no están atribuidos a personas físicas concretas.

6.7. La Universidad de Valladolid podrá bloquear el acceso y la visibilidad de una cuenta de su titularidad. Si, en presencia de un riesgo para la información contenida no fuera posible contar con permisos de acceso a la cuenta o su titular se negara a facilitar tal acceso, la Universidad podrá bloquear el acceso y la visibilidad de una cuenta de su titularidad. Asimismo, procederá a generar evidencia digital de la misma de acuerdo con lo previsto en su caso en las leyes vigentes. En todo caso, si del riesgo pudieran inferirse indicios de delito, los hechos se pondrán de inmediato en conocimiento de la autoridad judicial.

## 7. Normativa

En el uso del servicio del correo electrónico y con el objetivo de reducir los riesgos para la seguridad de la información y garantizar los derechos de las personas usuarias, deben aplicarse los preceptos que se detallan a continuación.

### RESPONSABILIDAD

7.1. Las personas usuarias son responsables de todas las actividades realizadas con sus cuentas de correo electrónico. En particular, se obligan al cumplimiento de las presentes normas. Cualquier conducta contraria a las Leyes, especialmente aquellas lesivas de derechos y libertades, podrá generar responsabilidad, sea esta disciplinaria o personal.



## Universidad de Valladolid

### NATURALEZA Y USOS DE LAS CUENTAS DE CORREO.

7.2. El correo electrónico es el medio institucional de comunicación oficial de la Universidad con la comunidad universitaria. El Reglamento de notificaciones y comunicaciones electrónicas de la UVa (2019), establece que la comunicación con las personas integrantes de la comunidad universitaria se realizará a través del correo electrónico corporativo proporcionado por la UVa. Asimismo, en la práctica de las notificaciones, la persona destinataria recibirá en su dirección de correo electrónico un aviso informativo comunicándole que tiene una notificación en la «Carpeta Ciudadana» de la sede electrónica.

7.3. Se recomienda limitar el uso del correo electrónico a fines de naturaleza académica, investigadora o administrativa. Minimizar el uso personal o privado permite reducir los riesgos y la carga que soportan los sistemas de información de la Universidad de Valladolid.

7.4. Se prohíbe el uso de cuentas de correo electrónico de otros proveedores para el desempeño de tareas vinculadas a las funciones que el usuario presta en la Universidad. En ese caso, los correos electrónicos se almacenarían y gestionarían en servidores de terceros sin ningún tipo de acuerdo con la Universidad de Valladolid, lo que imposibilitaría su control.

- Se incumpliría con la normativa sobre protección de datos.
- Podría comprometer información confidencial, datos de proyectos de investigación, secretos relacionados con la propiedad industrial, intelectual o comercial, etc.
- Se dificultaría la recuperación de la información en caso de necesidad, como en los supuestos de enfermedad grave, fallecimiento, comisión de actos delictivos, etc.

Asimismo, no se utilizarán este tipo de cuentas para el alta en servicios externos no contratados o no autorizados por la Universidad de Valladolid como el almacenamiento en la nube (*cloud*), encuestas, listas de correo electrónico o servicios equivalentes ofrecidos a particulares.

7.5. En ningún caso se configurará el identificador de usuario y contraseña de la Universidad de Valladolid en proveedores de servicios de correo electrónico de terceros. A modo de ejemplo, no se configurarán servicios como Gmail, Hotmail o similares para que consulten cuentas de correo electrónico de la UVa o para que envíen correos autenticados a través de los servidores de correo saliente de la UVa.

7.6. Las cuentas de correo electrónico institucional, y en particular, las vinculadas al desempeño de cargos o funciones representativas, no podrán ser utilizadas para fines personales o privados en ningún caso.

7.7. Las personas usuarias responderán personalmente del uso de las cuentas de correo electrónico de la Universidad de Valladolid con fines privados. Este uso no será admisible cuando se ejerza de manera abusiva, interfiera con el rendimiento propio del servicio, perjudique a la seguridad de los sistemas, suponga un alto coste o interfiera en las funciones que la propia persona tenga asignadas. Cualquier responsabilidad penal, civil o patrimonial que pudiera derivar de un uso de esta naturaleza corresponderá al usuario. En caso de detectarse usos



## Universidad de Valladolid

indebidos, la Universidad seguirá los correspondientes procedimientos administrativos o disciplinarios previstos. Si la información fuese requerida por Fuerzas y Cuerpos de Seguridad del Estado o autoridades judiciales, su entrega se hará con las máximas garantías.

7.8. Se prohíbe el uso de cuentas de correo electrónico de la Universidad de Valladolid como medio de registro o comunicación en servicios de la sociedad de la información. Los servicios como las redes sociales, entornos de comercio electrónico o aplicaciones móviles pueden generar riesgos adicionales a los sistemas de información de la Universidad de Valladolid. Cuando estos son atacados, exponen información de sus usuarios, lo que facilita acciones como el *spam*, el *phising* o el envío de software malicioso. Los usuarios de la Universidad deben contribuir a una reducción significativa de este riesgo, no usando su cuenta de correo de la Universidad como cuenta de registro o cambiándola allí donde eventualmente la usaran.

Esta recomendación no se aplica a servicios oficiales como, por ejemplo, el registro en instituciones con competencia en materia de calidad universitaria, Ministerios, CRUE, Comisión europea o equivalentes, así como para el desarrollo de funciones en que esté presente un interés público institucional.

7.9. La publicación de direcciones de correo electrónico en directorios o páginas web institucionales públicas o de la intranet de la Universidad de Valladolid no autoriza la remisión de mensajes para fines distintos de los autorizados. En particular, estos directorios no constituyen una fuente pública susceptible de ser utilizada para el envío de información publicitaria ni atribuye interés legítimo a cualquier tercero para usos distintos de los estrictamente vinculados a las finalidades administrativas o de gestión académica.

7.10. Utilizar el buzón de correo electrónico como almacenamiento no es una finalidad permitida por la Universidad de Valladolid. La capacidad de los servidores de correo electrónico de la Universidad de Valladolid es limitada. Cuando una cuenta se satura se restringen el envío y la recepción de mensajes. Por todo ello, se recomienda conservar en el buzón únicamente los mensajes imprescindibles y archivar en otro lugar toda la información que no se necesite en el buzón.

### NORMAS DE SEGURIDAD

7.11. Deben utilizarse contraseñas seguras. Para limitar la posibilidad de un acceso no autorizado a las cuentas de correo electrónico, es conveniente utilizar contraseñas robustas.

7.12. Deberá procederse al cambio de contraseñas siempre que el usuario sea requerido para ello por el sistema de información o por un responsable de seguridad.

7.13. Deben utilizarse protocolos seguros de comunicación. Para asegurar una comunicación confidencial con los servidores de correo electrónico de la UVa, es necesario configurar el cliente de correo electrónico para que utilice protocolos seguros, como POP3s, IMAPs para el correo entrante y SMTPs o SMTP con TLS para el correo saliente.

7.14. Es necesario utilizar los servidores de correo electrónico saliente centralizados de la Universidad de Valladolid. Para evitar en la medida de lo posible el envío de correo electrónico



## Universidad de Valladolid

infectado con software malicioso, es necesario que los servidores de correo saliente implementen mecanismos de detección. Para evitar su propagación, se recomienda que las conexiones de correo saliente requieran autenticación mediante usuario y contraseña. Para garantizar estos puntos, se recomienda configurar en su cliente de correo como servidor de correo saliente centralizado UVa: cartero.uva.es.

7.15. Se prohíbe ceder el uso de las cuentas de correo electrónico. Las cuentas de correo electrónico son personales e intransferibles. No se debe ceder el uso de la cuenta de correo a terceras personas, lo que podría provocar una suplantación de identidad y el acceso a información confidencial.

7.16. El envío o reenvío de correos electrónicos de forma masiva se limitará a los supuestos en los que resulte necesario por razón de la tarea que se realiza. Para el envío de correos electrónicos de carácter regular a un conjunto de destinatarios, se recomienda bien usar una lista de distribución cuando sea la herramienta idónea o, en su defecto, colocar la lista de direcciones en el campo de Copia Oculta (CCO o BCC), evitando su visibilidad a todos los receptores del mensaje.

Los envíos de correo electrónico masivo se regirán por los siguientes principios:

- Serán procedimientos usuales cuando su finalidad sea el envío de comunicaciones a colectivos determinados de la comunidad universitaria. Estos mensajes deberán ser autorizados por el responsable académico o administrativo competente.
- Se admite el uso de listas de correo electrónico siempre y cuando se utilicen para fines profesionales o académicos relacionados con el ámbito de funciones y competencias de la Universidad de Valladolid.

7.17. Debe revisarse la barra de direcciones antes de enviar un mensaje, confirmando la corrección del destinatario y evitando poner en copia visible en los casos de envíos con múltiples destinatarios. El envío de información a destinatarios erróneos puede suponer una brecha en la confidencialidad de la información. Cuando se responde a un mensaje es importante revisar las direcciones que aparecen en el campo "Con Copia" (CC). Además, deben borrarse todas las direcciones que pudieran aparecer en el correo enviado con anterioridad y que aparezcan reflejadas en el nuevo correo reenviado o respondido.

7.18. Preste atención al contenido de los mensajes que reenvía. Tenga en cuenta que los programas cliente de correo electrónico encadenan los correos enviados y sus respuestas. En determinadas circunstancias pueden contener información confidencial o sensible que no debería ser conocida por el destinatario del reenvío.

7.19. Deberá solicitarse autorización para la remisión masiva de correo electrónico a direcciones de correo electrónico publicadas en directorios o páginas web institucionales públicas o de intranet de la Universidad de Valladolid para fines específicos y legítimos de una persona usuaria. Así, por ejemplo, la difusión de eventos o actividades singulares, como



## Universidad de Valladolid

congresos o seminarios, o la realización de encuestas deberán tramitarse a través de los cauces institucionales.

7.20. No se permite enviar o reenviar cadenas de mensajes. Los mensajes alarmistas sobre virus o softwares maliciosos son, en muchas ocasiones, correos simulados (*hoax*) enviados en cadena, que pretenden saturar los servidores y la red. En caso de recibir un mensaje en cadena alertando de un virus o similar, se debe notificar la incidencia al Servicio de las Tecnologías de la Información y las Comunicaciones (en adelante STIC).

7.21. No debe responder a mensajes de *spam*. El término *spam* se define como el envío de correos electrónicos no solicitados de forma masiva. Constituye uno de los problemas de seguridad más habituales con los que se enfrentan las organizaciones. Tales mensajes pueden incluso contener código dañino que, de penetrar en los sistemas de información, podría comprometer su seguridad.

La mayor parte de los generadores de mensajes de *spam* se envían a direcciones de correo electrónico aleatoriamente generadas, esperando que las respuestas obtenidas confirmen la existencia de direcciones de cuentas reales. En ocasiones adoptan la apariencia de mensajes legítimos incluso llegando a contener información relativa a la Universidad de Valladolid que puede esperar.

En cualquier caso, nunca debe responderse a los mensajes de *spam*.

7.22. No debe utilizarse la cuenta correo electrónico de la Universidad y su contraseña para el registro en servicios de terceros. El uso de la dirección de correo electrónico en servicios ajenos puede comprometer su seguridad y la de la organización. El registro con la cuenta universitaria estaría justificado siempre que estos servicios estuviesen relacionados con la actividad profesional. En este caso, la contraseña de registro no deberá ser la misma que la de su cuenta de correo electrónico.

7.23. Se recomienda utilizar mecanismos de cifrado de la información. Los mensajes que contengan información sensible, confidencial o protegida deberán cifrarse, particularmente cuando se incluyan datos personales que puedan afectar a derechos y libertades de las personas. La contraseña que permita el descifrado, no se enviará por el mismo medio que el propio mensaje.

7.24. Es recomendable asegurarse de la identidad del remitente antes de abrir un mensaje. En numerosas ocasiones los ciberataques se originan cuando el atacante se hace pasar por una persona o entidad conocida del usuario receptor, como un amigo, compañero, entidad bancaria, etc.. El origen de estas acciones es diverso: acceso no autorizado a la cuenta, suplantación visual de la identidad, introducción de código malicioso que utiliza la cuenta remitente para propagarse, etc. Es importante tener en cuenta que resulta extremadamente sencillo enviar un correo electrónico con un remitente falso.



## Universidad de Valladolid

Nunca se debe confiar en que la persona con la que nos comunicamos vía correo electrónico sea quien dice ser, salvo en aquellos casos que se utilicen mecanismos de firma electrónica de los propios correos electrónicos y no sólo de los ficheros adjuntos.

En caso de recibir un correo sospechoso de esta naturaleza se recomienda:

- Ignorarlo y no abrirlo.
- En caso de percibir un riesgo grave, debe comunicar la incidencia de seguridad correspondiente al STIC.
- Nunca se debe responder ni reenviar un correo sospechoso. Si desea informar a la persona afectada, hágalo mediante un correo específico dirigido a su cuenta original.

7.25. No deben ejecutarse archivos adjuntos sospechosos. No deben ejecutarse los archivos adjuntos recibidos sin analizarlos previamente con la herramienta corporativa contra código malicioso. Esto es especialmente importante cuando se reciben adjuntos no solicitados o el correo electrónico recibido le ofrece algún tipo de duda.

Gran parte del código malicioso suele insertarse en ficheros adjuntos, ya sea en forma de ejecutables o en forma de macros de aplicaciones (Word, Excel, etc.). Asegúrese de que su Office está configurado para no ejecutar macros automáticamente.

7.26. En el acceso remoto vía web al correo electrónico, deben adoptarse las siguientes precauciones:

- Los navegadores utilizados para acceder al correo electrónico vía web deben estar permanentemente actualizados a su última versión, así como correctamente configurados.
- Una vez finalizada la sesión web, es obligatoria la desconexión con el servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada.
- Desactivar la interpretación de contenidos remotos a la hora de leer mensajes de correo utilizando clientes webmail.
- Desactivar las características de recordar contraseñas para el navegador.
- Activar la opción de borrado automático al cierre del navegador, de la información sensible registrada por el mismo: historial de navegación, descargas, formularios, caché, cookies, contraseñas, sesiones autenticadas, etc.

7.27. Se borrará del servidor de correo cualquier información sensible, confidencial o protegida. Esta podría ser accedida por un atacante, por lo que se aconseja su borrado una vez descargada.

7.28. Tenga en cuenta las siguientes recomendaciones adicionales:

- Evite acceder a su correo electrónico utilizando ordenadores de acceso público. Especialmente los de bibliotecas, hoteles, locutorios o cibercafés, etc.
- Desactivar la vista previa. Utilizar la vista previa para los correos de la bandeja de entrada comporta los mismos riesgos que abrirlos.



## Universidad de Valladolid

- Limitar el uso de HTML. El código malicioso puede encontrarse fusionado con el código HTML del mensaje. Desactivar la visualización HTML de los mensajes ayuda a evitar que el código malicioso se ejecute.
- Configurar el antivirus con la opción de analizar el correo. La utilización de herramientas tales como antivirus y cortafuegos ayuda a detectar el código malicioso y a mitigar sus efectos.
- No abrir correos electrónicos de *spam* o sospechosos. Aun cuando un mensaje no deseado hubiera traspasado el filtro contra *spam*, no debería abrirse, siendo conveniente informar sobre el correspondiente incidente de seguridad al STIC. Es recomendable borrar los correos sospechosos o, al menos, situarlos sin abrir en una zona de cuarentena.
- Informar de correos electrónicos con virus o software malicioso, sin reenviarlos. Si el usuario detectara que un correo electrónico contiene un virus o, en general, código malicioso, conviene notificar el incidente de seguridad al STIC y no reenviarlo, para evitar su posible propagación.

### PIE DE FIRMA EN CUENTAS DE CORREO ELECTRÓNICO CORPORATIVO

7.29. Los remitentes de correo electrónico corporativo deben identificarse. Se incluirá en el pie del correo electrónico la identificación de la persona y cargo que envía el mensaje. Se seguirán las normas de estilo que indique la Universidad de Valladolid. De forma general, puede utilizarse un generador de firmas. Si un área funcional cuenta con diseño de firma y logo distintivo propio, puede utilizarlo.

7.30. Se añadirá al pie los correos electrónicos una cláusula sobre confidencialidad y protección de datos. Esta será idéntica a la que proporcione el generador automatizado.

*Este mensaje puede contener información confidencial, sometida al secreto profesional, cuya divulgación no está permitida por la ley. Si usted no es su destinatario, por favor, notifíquelo al remitente y borre este correo de su sistema. A los efectos de la protección de datos y el RGPD, consulte: [protección de datos en la UVa](#). El emisor no garantiza la integridad, rapidez o seguridad del presente correo, ni se responsabiliza de posibles perjuicios derivados de la captura, incorporaciones de virus o cualesquiera otras manipulaciones efectuadas por terceros.*

*This message may contain confidential information covered by the obligation of professional secrecy, the disclosure of which would be contrary to the law. If you are not the intended recipient, please advise the sender and delete this e-mail from your system. For the purposes of data protection and GDPR, read: [UVa data protection](#). The sender does not guarantee the integrity, the accuracy, the swift delivery or the security of this e-mail transmission, and assumes no responsibility for any possible damage incurred through data capture, virus incorporation or any manipulation carried out by third parties.*

7.31. Finalización de la relación laboral o académica. El correo electrónico constituye una herramienta de trabajo o aprendizaje puesta a disposición de los miembros de la comunidad universitaria. Con la extinción de la relación jurídica con la Universidad, sea laboral o académica,



## Universidad de Valladolid

el buzón de correo electrónico podría ser clausurado. Debe consultar, dependiendo del colectivo al que pertenezca, la posibilidad de conservación del mismo.

### 8. Testamento digital

8.1. Se facilitará acceso a los buzones de las cuentas de correo electrónico de personas fallecidas. Puede hacerse, previa solicitud por:

- a) Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos. Como excepción, las personas mencionadas no podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley.
- b) El albacea testamentario, así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello.
- c) En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.
- d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

8.2. La condición que legitima el acceso a la cuenta exigirá determinadas condiciones. En particular:

- a) Acreditación de la condición de heredero mediante certificado expedido por el Ministerio de Justicia y copia del testamento, o cualquier condición testamentaria que habilite para el citado acceso.
- b) Declaración judicial que declare la sucesión 'ab intestato'.
- c) Cuando pudiera existir en el correo información relacionada con derechos de propiedad intelectual, secreto y confidencialidad, secreto industrial, patentes, marcas u otros derechos equivalentes, deberá acreditarse la titularidad sobre los mismos.

8.3. Las solicitudes irán dirigidas al Secretario General de la Universidad de Valladolid acompañadas de la documentación indicada.

8.4. Una vez realizadas las comprobaciones documentales que acrediten la legitimación para el acceso a la información, la Secretaría General oficiará al STIC autorizando el acceso. El STIC realizará las siguientes tareas:

- a) Se generarán dos copias del buzón de correo. Una se pondrá a disposición de la persona solicitante y la otra quedará reservada, bloqueada y únicamente a disposición de jueces y tribunales o para la resolución de posibles controversias durante un periodo máximo de



## Universidad de Valladolid

5 años.

- b) Se accederá bajo la supervisión de un técnico autorizado a la carpeta denominada “personal” y en su caso, a la carpeta denominada “confidencial” cuando se acredite la titularidad de los derechos en los términos del párrafo 8.2.c).
- c) La información ubicada en cualesquiera otras carpetas y en la bandeja de entrada se presumirá de titularidad de la Universidad de Valladolid. En cualquier caso, el técnico habilitado podrá verificarla diferenciando la información privada de la corporativa. Aquella será separada de esta última.
- d) Una vez realizada la copia de seguridad se procederá a eliminar la cuenta de correo, suprimir el espacio en disco o bloquear el perfil, o al borrado del terminal (ordenador, tableta, *smartphone*, etc.) o soporte.
- e) La copia se entregará mediante oficio en el que se acuse recibo de la información entregada. Salvo que resulte imposible por su volumen, se incluirá en el oficio algún resumen, descripción o pantallazo informativo relativo al soporte que indique su contenido. El documento de entrega deberá registrarse en su salida.
- f) Concluido el procedimiento, se archivará la copia en el STIC, trasladándose el original a la Secretaría General, junto con cualquier documento o trámite adicional relevante, para su integración en el expediente.

En coherencia con el valor de la igualdad de género asumido por la Universidad, todas las denominaciones que en esta Norma se efectúan en género masculino, cuando no hayan sido sustituidas por términos genéricos, se entenderán hechas indistintamente en género femenino.