I. DISPOSICIONES Y ACUERDOS

I.2. Consejo de Gobierno

Acuerdo 2/2022, del Consejo de Gobierno de la Universidad Internacional de Andalucía, de 28 de enero de 2022, por el que se aprueba la modificación de la Normativa de Seguridad de la Información.

El Consejo de Gobierno de la Universidad Internacional de Andalucía, reunido en sesión ordinaria de 28 de enero de 2022, aprueba la modificación de la Normativa de Seguridad de la Información.

NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN

Aprobado por Consejo de Gobierno el 5 de febrero de 2019.

Modificado por Consejo de Gobierno el 28 de enero de 2022.

Índice

1 Objeto

Los Sistemas de Información constituyen elementos básicos para el desarrollo de las misiones encomendadas a la Universidad Internacional de Andalucía, por lo que los usuarios deben utilizar estos recursos de manera que se preserven en todo momento las dimensiones de la seguridad sobre las informaciones manejadas y los servicios prestados.

La utilización de equipamiento informático y de comunicaciones es actualmente una necesidad en cualquier organización. Estos medios y recursos se ponen a disposición de los usuarios como instrumentos de trabajo para el desempeño de su actividad profesional, razón por la cual compete a la Universidad Internacional de Andalucía determinar las normas, condiciones y responsabilidades bajo las cuales se deben utilizar tales recursos tecnológicos.

Por tanto, la presente Normativa de Seguridad de la Información de la Universidad Internacional de Andalucía tiene como objetivo establecer normas encaminadas a alcanzar la mayor eficacia y seguridad en su uso.

2 Alcance

Esta Normativa es de aplicación a todo el ámbito de actuación de la Universidad Internacional de Andalucía, y sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información.

La presente Normativa es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la Universidad Internacional de Andalucía, incluyendo el personal de proveedores externos, cuando sean usuarios de los Sistemas de Información de la Universidad Internacional de Andalucía.

En el ámbito de la presente normativa, se entiende por usuario cualquier empleado perteneciente o ajeno a la Universidad Internacional de Andalucía, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con la Universidad Internacional de Andalucía y que utilice o posea acceso a los Sistemas de Información de la Universidad Internacional de Andalucía.

3 Vigencia

La presente Normativa de Seguridad de la Información de la Universidad Internacional de Andalucía ha sido aprobada por Acuerdo del Consejo de Gobierno de la Universidad Internacional de Andalucía de 5 de febrero de 2019, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la Universidad Internacional de Andalucía pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la Universidad Internacional de Andalucía.

4 Revisión y evaluación

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

- 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 (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Comité de Seguridad revisará la presente Normativa, que se someterá, de haber modificaciones, a la aprobación del Consejo de Gobierno de la Universidad Internacional de Andalucía.
- 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, etc.
- Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

5 Utilización del equipamiento informático y de comunicaciones

La Universidad Internacional de Andalucía facilita a los usuarios que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional. Así pues, los datos, dispositivos, programas y servicios informáticos que la Universidad Internacional de Andalucía pone a disposición de los usuarios deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales. Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido.

En general, el ordenador personal (PC) será el recurso informático que permitirá el acceso de los usuarios a los Sistemas de Información y servicios informáticos de la Universidad Internacional de Andalucía, constituyendo un elemento muy importante en la cadena de seguridad de los sistemas de información, razón por la que es necesario adoptar una serie de precauciones y establecer normas para su adecuada utilización.

Este apartado concierne específicamente a todos los equipos facilitados por la Universidad Internacional de Andalucía para su utilización por parte de los usuarios, incluyendo equipos de sobremesa, portátiles y dispositivos móviles con capacidades de acceso a los Sistemas de Información de la organización.

5.1 Normas generales

- Los ordenadores personales deberán utilizarse únicamente para fines corporativos y como herramienta de apoyo a las competencias profesionales de los usuarios autorizados.

- Únicamente el personal autorizado podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos, especialmente en aquellos aspectos que puedan repercutir en la seguridad de los Sistemas de Información de la Universidad Internacional de Andalucía. Cuando se precise instalar dispositivos no provistos por la Universidad Internacional de Andalucía deberá solicitarse autorización previa al Área de Gestión de las TICs.

- Está prohibido alterar, sin la debida autorización, cualquiera de los componentes físicos o lógicos de los equipos informáticos y dispositivos de comunicación, salvo autorización expresa del Área de Gestión de las TICs.

- Salvo autorización expresa del Área de Gestión de las TICs, los usuarios no tendrán privilegio de administración sobre los equipos.

- Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento. Este acceso se limitará únicamente a las acciones necesarias para el mantenimiento o la resolución de problemas que pudieran encontrarse en el uso de los recursos informáticos y de comunicaciones, y finalizará completado el mantenimiento o una vez resueltos aquellos.

- Si el personal de soporte técnico detectase cualquier anomalía que indicara una utilización de los recursos contraria a la presente norma, lo pondrá en conocimiento del Responsable de Seguridad, que tomará las oportunas medidas correctoras.

- Los ordenadores personales de la organización deberán mantener actualizados los parches de seguridad de todos los programas que tengan instalados. Se deberá prestar especial atención a la correcta actualización, configuración y funcionamiento del S.O. y antivirus corporativo.

- Los usuarios deberán notificar al Centro de Atención a Usuarios (CAU), a la mayor brevedad posible, cualquier comportamiento anómalo de su ordenador personal, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo.

- El usuario debe ser consciente de las amenazas provocadas por malware. Muchos virus y troyanos requieren la participación de los usuarios para propagarse, ya sea a través de dispositivos de almacenamiento de datos externos (disquetes, CDs/DVDs, memorias USB, etc.), mensajes de correo electrónico o instalación de programas descargados desde Internet. Es imprescindible, por tanto, vigilar el uso responsable los equipos para reducir este riesgo.

- El usuario será responsable de toda la información extraída fuera de la organización a través de dispositivos que le hayan sido asignados, sea cual sea el medio utilizado para ello (memorias USB, CDs, almacenamiento en la nube, etc.). Es imprescindible un uso responsable de los mismos, especialmente cuando se trate información sensible, confidencial o protegida.

- El cese de actividad de cualquier usuario debe ser comunicada de forma oficial e inmediata al Área de Gestión de las TICs, al objeto de que le sean retirados los recursos informáticos que le hubieren sido asignados. Correlativamente, cuando los medios informáticos o de comunicaciones proporcionados por la Universidad Internacional de Andalucía estén asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tendrá que devolverlos inmediatamente a la unidad responsable cuando finalice su vinculación con dicho puesto o función.

5.2 Usos específicamente prohibidos

Están terminantemente prohibidos los siguientes comportamientos:

- Utilización de cualquier tipo de software dañino.
- Utilización de programas que, por su naturaleza, hagan un uso abusivo de la red.
- Conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por la Universidad Internacional de Andalucía, sin la previa autorización del Área de Gestión de las TICs.
- Utilización de conexiones y medios inalámbricos con tecnologías WiFi, Bluetooth, etc. que no estén autorizados previamente por la Universidad Internacional de Andalucía.
- Utilización de dispositivos USB, teléfonos móviles u otros elementos, como acceso alternativo a Internet, salvo autorización y solicitud expresa del Área de Gestión de las TICs.
- Instalación y/o utilización de programas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual. Este comportamiento estará sometido a las previsiones disciplinarias, administrativas, civiles o penales descritas en las leyes.

5.3 Normas específicas para equipos portátiles y móviles

- Los equipos portátiles y móviles serán asignados por el Área de Gestión de las TICs a petición del Responsable de Área correspondiente.
- Existirá un inventario actualizado de los equipos portátiles y móviles. El Área de Gestión de las TICs deberá ser informado de dicho inventario, así como de los cambios que se produzcan en él.
- Este tipo de dispositivos estará bajo la custodia del usuario que los utilice, quién deberá adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas.
- La sustracción de estos equipos se ha de poner inmediatamente en conocimiento del Área de Gestión de las TICs para la adopción de las medidas de seguridad que correspondan. Igualmente se deberá informar al área que le corresponda la gestión del inventario para que pueda proceder a la actualización del mismo.

- Los equipos portátiles y móviles deberán utilizarse únicamente para fines institucionales, especialmente cuando se usen fuera de las instalaciones de la Universidad Internacional de Andalucía.

- Los usuarios de estos equipos se responsabilizarán de que no serán usados por terceras personas ajenas a la Universidad Internacional de Andalucía o no autorizadas para ello.

- Los usuarios de equipos portátiles deberán realizar conexiones periódicas a la red corporativa, según las instrucciones proporcionadas por la Universidad Internacional de Andalucía, para permitir la actualización de aplicaciones, sistema operativo, firmas de antivirus y demás medidas de seguridad.

- Cuando la tipología de la información tratada así lo requiera, los ordenadores portátiles afectados deberán tener cifrado el disco duro, disponer de software que garantice un arranque seguro, así como mecanismos de auditoría capaces de crear un registro por cada fichero extraído del sistema por cualquier medio (red, dispositivos extraíbles, impresoras, etc.).

- Los usuarios no tendrán privilegio de administración sobre los equipos portátiles, teniendo prohibido realizar cualquier modificación hardware/software sobre los mismos. Corresponderá al Área de Gestión de las TICs llevar a cabo estas modificaciones.

5.4 Uso de soportes de almacenamiento de datos externos

- Con carácter general, el uso de soportes de almacenamiento de datos externos (memorias USB, CDs/DVDs, tarjetas de memoria, etc) en la Universidad Internacional de Andalucía no está autorizado. En el caso de ser necesaria su uso, deberá justificarse formalmente por el usuario y requerirá la previa autorización del Responsable de Área y el Área de Gestión de las TICs.

- En el caso excepcional en el que a un usuario se le autorice el uso de dichos soportes, se recuerda que están destinadas a un uso exclusivamente profesional, como herramienta de transporte de ficheros, no como herramienta de almacenamiento. La Universidad Internacional de Andalucía podrá poner a disposición de los usuarios unidades de almacenamiento en red, que podrán usarse para tal propósito.

- Una vez finalizado el proceso de intercambio de ficheros, se deberá proceder al borrado o destrucción del contenido de dicho soporte de almacenamiento.

- La pérdida o sustracción del soporte de almacenamiento deberá ponerse en conocimiento del Área de Gestión de las TICs, de forma inmediata con indicación de su contenido.

5.5 Impresoras en red y fotocopiadoras

- Con carácter general, deberán utilizarse las impresoras en red y las fotocopiadoras corporativas. Excepcionalmente, podrán instalarse impresoras locales, gestionadas por un puesto de trabajo de usuario. En este caso, la instalación irá precedida de la autorización pertinente por parte del responsable del peticionario. En ningún caso el usuario podrá hacer uso de impresoras, fotocopiadoras o equipos de fax que no hayan sido proporcionados por la Universidad Internacional de Andalucía y, en su consecuencia, estén debidamente inventariados.

- Cuando se imprima documentación, deberá permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.

- Conviene no olvidar tomar los originales de la fotocopiadora, una vez finalizado el proceso de copia. Si se encontrase documentación sensible, confidencial o protegida abandonada en una fotocopiadora o impresora, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. Caso de desconocer a su propietario o no localizarlo, deberá notificarse como un incidente de seguridad.

5.6 Digitalización de documentos

- Con carácter general, cuando se digitalicen documentos el usuario deberá ser especialmente cuidadoso con la selección del directorio compartido donde habrán de almacenarse las imágenes obtenidas, especialmente si contienen información sensible, confidencial o protegida.

- Conviene no olvidar tomar los originales del escáner, una vez finalizado el proceso de digitalización. Si se encontrase documentación sensible, confidencial o protegida abandonada en un escáner, el usuario intentará localizar a su propietario para que éste la recoja inmediatamente. Caso de desconocer a su propietario o no localizarlo, lo notificará inmediatamente como un incidente de seguridad.

5.7 Protección de equipos y puestos de trabajo

- Los puestos de trabajo del personal deben ubicarse preferentemente en ubicaciones que no queden expuestas al acceso de personas externas. No será de aplicación esta norma en el caso de equipos que estén destinados al uso público.

- Los puestos ubicados en zonas de atención o tránsito de público, deben situarse de forma que las pantallas no puedan ser visualizadas por personas externas.

- Los puestos de trabajo permanecerán despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.

- Al finalizar la jornada de trabajo, los usuarios deben guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno.

- Cada vez que un usuario se ausente de su lugar de trabajo debe bloquear su puesto de usuario, de forma que se proteja el acceso a las aplicaciones y servicios. Adicionalmente, los puestos de trabajo se configurarán para bloquearse automáticamente tras un periodo de 10 minutos de inactividad.

5.8 Cuidado y protección de la documentación impresa

- Antes de imprimir documentos, el usuario debe asegurarse de que es absolutamente necesario hacerlo. La documentación impresa que contenga datos sensibles, confidenciales o protegidos, debe ser especialmente resguardada, de forma que sólo tenga acceso a ella el personal autorizado, debiendo ser recogida rápidamente de las impresoras y fotocopiadoras.

- Si, una vez impresa, es necesario almacenar tal documentación, el usuario habrá de asegurarse de proteger adecuadamente y bajo llave aquellas copias que contengan información sensible, confidencial o protegida.

- Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser eliminados en las máquinas destructoras de la Universidad Internacional de Andalucía de forma que no sea recuperable la información que pudieran contener.

5.9 Pizarras

- Antes de abandonar las salas o permitir que alguien ajeno entre, se limpiarán adecuadamente las pizarras de las salas de reuniones o despachos, cuidando que no quede ningún tipo de información sensible o que pudiera ser reutilizada.

5.10 Protección de la dignidad de las personas

- Está terminantemente prohibida toda transmisión, distribución o almacenamiento de cualquier material obsceno, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas.

6 Identificación y autenticación

- Los usuarios dispondrán de un código de usuario (user-id) y una contraseña (password) o bien una tarjeta criptográfica con certificado digital, para el acceso a los Sistemas de Información de la Universidad Internacional de Andalucía, y son responsables de la custodia de los mismos y de toda actividad relacionada con el uso de su acceso autorizado. El código de usuario es único para cada persona en la organización, intransferible e independiente del PC o terminal desde el que se realiza el acceso.

- Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales de acceso o tarjeta criptográfica a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros.

- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.

- Si un usuario tiene la certeza o sospechas fundadas de que sus credenciales están siendo utilizadas por otra persona, deberá proceder a la comunicación inmediata del correspondiente incidente de seguridad.

- Los usuarios deben utilizar contraseñas seguras de acuerdo a la política de calidad de contraseñas establecidas en la Universidad Internacional de Andalucía. Las contraseñas no deben estar compuestas únicamente por palabras del diccionario u otras fácilmente predecibles o asociables al usuario (nombres de su familia, direcciones, matrículas de coche, teléfonos, nombres de productos comerciales u organizaciones, identificadores de usuario, de grupo o del sistema, DNI, etc.).

- Si, en un momento dado, un usuario recibiera una petición solicitando sus credenciales (independientemente del medio utilizado para ello, llamada telefónica, email, ...) deberá negarse a proporcionar dichos datos, se considerará una incidencia de seguridad y por lo tanto deberá informar de este hecho inmediatamente.

7 Medidas de protección de infraestructuras

Todas aquellas salas que alberguen infraestructura (principalmente servidores y equipos de comunicaciones) que de soporte a los sistemas de información de la Universidad Internacional de Andalucía deberán cumplir, al menos, las siguientes medidas de protección física:

- Áreas separadas y con control de acceso: el equipamiento se instalará en áreas específicas para su función, de manera que sea posible controlar los accesos a las áreas indicadas.

- Identificación de las personas: se identificará a todas las personas que accedan a los locales y se mantendrá un registro de todas las entradas y salidas de personas.
- Acondicionamiento de los locales: deberán disponer de adecuadas condiciones de temperatura y humedad, para lo que se dispondrán medidas de monitorización y control. El cableado debe estar protegido frente a incidentes fortuitos o deliberados.
- Energía eléctrica: se garantizará el suministro eléctrico de los sistemas en caso de fallo del suministro genera, garantizando el tiempo suficiente para una terminación ordenada de los procesos, salvaguardando la información. Al menos, deberán disponer de Sistemas de Alimentación ininterrumpida (S.A.I.).
- Protección frente a incendios e inundaciones: los locales se protegerán frente a incendios e inundaciones con origen fortuito o deliberado.
- Registro de entrada y salida de equipamiento: se llevará un registro detallado de toda entrada y salida de equipamiento, incluyendo la identificación de la persona que autoriza el movimiento.

8 Acceso de terceros a los edificios

Los terceros ajenos a la Universidad Internacional de Andalucía que, eventualmente, permanecieran en sus edificios, instalaciones o dependencias, deberán observar las siguientes normas:

- El personal ajeno a la Universidad Internacional de Andalucía que temporalmente deba acceder a los Sistemas de Información de la Universidad Internacional de Andalucía, deberá hacerlo siempre bajo la supervisión de algún miembro acreditado de la Universidad Internacional de Andalucía (responsable).
- Cualquier incidente que surja antes o en el transcurso del acceso a la Universidad Internacional de Andalucía deberá ponerlo en conocimiento de su responsable.
- Para los accesos de terceros a los sistemas de información de la Universidad Internacional de Andalucía, siempre que sea posible, se les crearán usuarios temporales que serán eliminados una vez concluido su trabajo en la Universidad Internacional de Andalucía. Si, de manera excepcional, tuvieran que utilizar identificadores de usuarios ya existentes, una vez finalizados dichos trabajos, se procederá al cambio inmediato de las contraseñas de los usuarios utilizados.

- Tales personas, en lo que les sea de aplicación, deberán cumplir puntualmente la presente Normativa General, así como el resto de normativa de seguridad de la Universidad Internacional de Andalucía.

- Para acceder a los edificios, instalaciones o dependencias de la Universidad Internacional de Andalucía deberá estar en posesión de la correspondiente documentación de identificación personal admitida en Derecho (DNI., pasaporte, etc.), debiendo estar incluido en la relación nominal proporcionada previamente por la empresa a la que perteneciere. La primera vez que acceda físicamente deberá identificarse y solicitar la presencia de la persona responsable de la Universidad Internacional de Andalucía, que constituirá su enlace durante su estancia en él.

- Una vez en el interior de los edificios, dependencias o instalaciones de la Universidad Internacional de Andalucía, los terceros sólo tendrán autorización para permanecer en el puesto de trabajo que les haya sido asignado y en las zonas de uso común

- Asimismo, deberán tener autorización del responsable cuando tengan necesidad de realizar desplazamientos entre distintos departamentos de la Universidad Internacional de Andalucía.

- Los terceros atendrán siempre a los requerimientos que le hiciere el personal de seguridad de los edificios, instalaciones o dependencias a los que tuvieren acceso.

9 Uso del correo electrónico corporativo

El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición de los usuarios de la Universidad Internacional de Andalucía, para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas.

Se trata de un recurso compartido por todos los usuarios de la organización, por lo que un uso indebido del mismo repercute de manera directa en el servicio ofrecido a todos.

Por ello, se dictan las siguientes normas de uso.

9.1 Normas generales

- Todos los usuarios que lo precisen para el desempeño de su actividad profesional, dispondrán de una cuenta de correo electrónico, para el envío y recepción de mensajes internos y externos a la organización, es importante recordar que no se debe utilizar el correo electrónico como espacio de almacenamiento.

- Únicamente podrán utilizarse las herramientas y programas de correo electrónico suministrados, instalados y configurados por la Universidad Internacional de Andalucía.

- El correo corporativo deberá utilizarse, única y exclusivamente, para la realización de las funciones encomendadas al personal, evitando el uso privado del mismo. En ningún momento debe usarse como un medio de difusión masiva e indiscriminada de información. Los usuarios son responsables de todas las actividades realizadas con las cuentas de correo electrónico proporcionadas por la Universidad.

- Revisar la barra de direcciones antes de enviar un mensaje para comprobar que no hay destinatarios erróneos y evitar una brecha en la confidencialidad de la información.

- Usar el campo Copia Oculta (CCO o BCCO) para evitar la visibilidad de direcciones de correo a todos los receptores de un mensaje cuando el usuario tenga necesidad de enviarlo a un conjunto de destinatarios.

- La utilización de correos electrónicos dirigidos a la totalidad del personal de la Universidad Internacional de Andalucía o a colectivos o grupos de la UNIA, deberá ser autorizada por el Rector o en quien delegue las competencias de comunicación. Ningún usuario tendrá acceso al envío de correos masivos sin la correspondiente autorización.

- Las vías de comunicación mediante soporte virtual de la representación sindical con los trabajadores serán objeto de negociación con la finalidad de establecer unos adecuados canales de información entre dicha representación y los trabajadores y trabajadoras de la Universidad Internacional de Andalucía, y en todo caso, el envío de correos masivos al personal estará sometido a lo previsto en el apartado anterior.

- El acceso al contenido del correo electrónico del personal de la Universidad de Andalucía es personal e intransferible, nadie puede acceder al correo personal de ningún miembro de la Universidad, salvo por orden del Rector en cumplimiento de mandamiento judicial. La contravención de esta norma dará lugar a la denuncia del infractor ante las autoridades judiciales competentes.

- Se deberá notificar como un incidente de seguridad cualquier tipo de anomalía detectada, así como un alto volumen de correos no deseados (spam) que se reciban, a fin de configurar adecuadamente las medidas de seguridad oportunas.

- Se deberá prestar especial atención a los ficheros adjuntos en los correos recibidos. No deben abrirse ni ejecutarse ficheros de fuentes no fiables, puesto que podrían contener virus o código malicioso. En caso de duda sobre la confiabilidad de los mismos, se recomienda borrar el mensaje o situarlo en cuarentena hasta disponer de más datos, especialmente si contiene ficheros adjuntos. Se deberá notificar esta circunstancia como un incidente de seguridad.

- Está terminantemente prohibido suplantar la identidad de un usuario de internet, correo electrónico o cualquier otra herramienta colaborativa.

- Para verificación y monitorización, los datos de conexión y tráfico se guardarán en un registro durante el tiempo que establezca la normativa vigente en cada supuesto. En ningún caso esta retención de datos afectará al secreto de las comunicaciones.

9.2 Usos especialmente prohibidos

Las siguientes actuaciones están explícita y especialmente prohibidas:

- El envío de correos electrónicos con contenido inadecuado, ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad, discapacidad, que contengan programas informáticos (software) sin licencia, que vulneren los derechos de propiedad intelectual de los mismos, de alerta de virus falsos o difusión de virus reales y código malicioso, o cualquier otro tipo de contenidos que puedan perjudicar a los usuarios, identidad e imagen corporativa y a los propios sistemas de información de la organización.

- El acceso a un buzón de correo electrónico distinto del propio y el envío de correos electrónicos con usuarios distintos del propio.

- La difusión de la cuenta de correo del usuario en listas de distribución, foros, servicios de noticias, etc., que no sean consecuencia de la actividad profesional del usuario.

- Responder mensajes de los que se tenga sospechas sobre su autenticidad, confiabilidad y contenido, o mensajes que contengan publicidad no deseada. Responder a SPAM

- La utilización del correo corporativo como medio de intercambio de ficheros especialmente voluminosos sin autorización, y el envío de información sensible, confidencial o protegida.

10 Acceso a internet y otras herramientas de colaboración

El acceso corporativo a Internet es un recurso centralizado que la Universidad Internacional de Andalucía pone a disposición de los usuarios, como herramienta necesaria para el acceso a contenidos y recursos de Internet y como apoyo al desempeño de su actividad profesional.

La Universidad Internacional de Andalucía velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y productividad del personal, como desde los riesgos de seguridad asociados a su uso.

10.1 Normas generales

- Las conexiones que se realicen a Internet deben obedecer a fines profesionales, teniendo siempre en cuenta que se están utilizando recursos informáticos restringidos y escasos. El acceso a Internet para fines personales debe limitarse y, de ser absolutamente necesario, sólo debe utilizarse un tiempo razonable, que no interfiera en el rendimiento profesional ni en la eficiencia de los recursos informáticos corporativos.

- Sólo se podrá acceder a Internet mediante el navegador suministrado y configurado por la Universidad Internacional de Andalucía en los puestos de usuario. No podrá alterarse la configuración del mismo ni utilizar un navegador alternativo, sin la debida autorización del Área de Gestión de las TICs.

- Deberá notificarse al Centro de Atención a Usuarios de la Universidad Internacional de Andalucía (CAU) cualquier anomalía detectada en el uso del acceso a Internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso.

10.2 Usos específicamente prohibidos

Quedan prohibidas las siguientes actuaciones:

- La descarga de archivos muy voluminosos, especialmente en horarios coincidentes con la atención al público, salvo autorización expresa.

- La descarga de programas informáticos o ficheros con contenido dañino que supongan una fuente de riesgos para la organización.

- El acceso a recursos y páginas-web, o la descarga de programas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.

- La utilización de aplicaciones o herramientas (especialmente, el uso de programas de intercambio de información, P2P) para la descarga masiva de archivos, programas u otro tipo de contenido (música, películas, etc.).

11 Normativa en materia de uso de redes sociales

Los siguientes epígrafes recogen el conjunto de medidas que deben tenerse en cuenta cuando se use o se pretendan usar las Redes Sociales como herramienta de comunicación y difusión de las funciones competencialmente de la Universidad Internacional de Andalucía.

11.1 Autorización previa

Con carácter general, y salvo las excepciones que pudieran autorizarse en la Universidad Internacional de Andalucía, y que, en todo caso, deberán estar recogidas en la Política de Seguridad institucional, ninguna persona que preste sus servicios en la Universidad Internacional de Andalucía podrá darse de alta en ninguna red social, en nombre o en representación de la Universidad Internacional de Andalucía, salvo autorización expresa de Secretaría General con el conocimiento del Responsable de Seguridad.

Por tanto, salvo en el supuesto señalado, la presencia en las redes sociales de un empleado público de la Universidad Internacional de Andalucía será siempre a título personal.

11.2 Medidas comportamentales

Una vez autorizado a darse de alta en una red social en representación de la Universidad Internacional de Andalucía, el empleado público usuario de la red social de que se trate debe observar las siguientes normas de comportamiento:

- Recordar en todo momento que las redes sociales constituyen un foro público. Por tanto, por el hecho de agregar cualquier dato, comentario o información, el usuario está asumiendo que éste puede ser visto por los restantes usuarios de tal social, por la Universidad Internacional de Andalucía y, en general, por cualquier persona.

- Si el usuario está usando el perfil de la red social en representación de la Universidad Internacional de Andalucía, conviene mostrar abiertamente tal representación, a menos que existan circunstancias excepcionales que no lo aconsejen, tales como una amenaza potencial a la seguridad personal. En cualquier caso, nunca deben proporcionarse detalles personales tales como la dirección o los números de teléfono personales.

- Es siempre recomendable hablar en primera persona, tratando de aportar valor en los comentarios vertidos, facilitando informaciones y perspectivas contrastadas y que no se encuentren tipificadas como información clasificada o cuya revelación pudiera ocasionar un perjuicio a la Universidad Internacional de Andalucía o, en general, a cualquier persona o entidad, pública o privada. El usuario debe recordar que será siempre responsable de sus aportaciones y de las eventuales consecuencias en su reputación y, por ende, en la de la Universidad Internacional de Andalucía en el que presta sus servicios. En caso de dudas, lo mejor es abstenerse de hacer una contribución.

  En el orden jurídico, no olvidemos que el art. 53.3 del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público, señala que las actuaciones de los empleados públicos se ajustarán a los principios de lealtad y buena fe con la Administración en la que presten sus servicios, y con sus superiores, compañeros, subordinados y con los ciudadanos.

- Las redes sociales deben constituir un foro de intercambio de opiniones o para el debate constructivo, pero no es el ámbito apropiado para crear polémica, descalificar a otras personas o a terceros, ni para presentar quejas y reclamaciones que deben canalizarse a través de las vías específicas que la Administración Pública y la propia Universidad Internacional de Andalucía tiene establecidas para esa finalidad.

- El usuario debe tratar con respeto a los otros usuarios, usando un lenguaje apropiado y correcto y actuando siempre como si estuviera en presencia de la(s) otra(s) persona(s).

- Salvo autorización, el usuario no debe publicar material publicitario ni comunicacional de la Universidad Internacional de Andalucía, ni debe hacer uso de su perfil en la red social para lucrarse o hacer negocio, ni para comparar las funciones, competencias o, en general, desenvolvimiento de la Universidad Internacional de Andalucía con otras entidades.

- Los contenidos publicados en las redes sociales pueden estar sujetos a Derechos de Propiedad Intelectual, por lo que la publicación de cualquier contenido requiere tener la certidumbre de que se encuentra libre de estas cargas.

- La contribución del usuario en la red social debe presentar datos reales, concretos y argumentación consistente. Se permiten citas o la reproducción de pequeños fragmentos de textos, libros u obras de terceros en general, siempre y cuando se indique la fuente y el nombre del autor. Si el usuario realiza una contribución propia (texto, fotografías, gráficos, vídeos o audios) debe saber que otorga a la Universidad Internacional de Andalucía autorización para reproducirla en cualquier medio físico o virtual donde se indicará el nombre del empleado público como autor, todo ello sin perjuicio de que otros usuarios también podrían guardarlos o reproducirlos.

- El logotipo de la Universidad Internacional de Andalucía y, en general, cualquier otro logotipo o distintivo gráfico de la Universidad Internacional de Andalucía o de cualquier entidad del Sector Público constituyen marcas registradas. También son titularidad de la Universidad Internacional de Andalucía los contenidos colgados en su portal o sede electrónica y, por tanto, la Universidad Internacional de Andalucía se reserva todos los derechos de propiedad intelectual e industrial asociados a los mismos. El usuario debe comprometerse a respetarlos y a no utilizarlos sin la debida autorización, cualquiera que sea el medio.

- La descarga de contenidos, su copia o impresión requerirá autorización del superior del empleado (Jefe de Área, Servicio o Departamento).

- En ningún caso deberá usarse la red social para el intercambio de credenciales o contraseñas, de cualquier sistema y para cualquier finalidad.

- La información contenida en el perfil de la red social no deberá considerarse nunca como información oficial en relación con las funciones y competencias de la Universidad Internacional de Andalucía, en los términos que puedan estar reservados a las funciones de la sede electrónica de la Universidad Internacional de Andalucía, según dispone el art. 38 de la Ley 40/2015.

- El perfil de la red social de que se trate puede contener manifestaciones sobre previsiones o estimaciones que incluyen comentarios sobre el desarrollo de las funciones de la Universidad Internacional de Andalucía basadas en juicios actuales, pudiendo suceder que determinados riesgos, incertidumbres y otros factores

relevantes, desconocidos o imprevisibles ocasionen que los resultados difieran materialmente de lo esperado. El usuario debe recordar que las declaraciones relativas a los resultados, funciones, competencias, etc., no pretenden dar a entender que el desempeño de la Universidad Internacional de Andalucía será necesariamente el previsto. Nada en el perfil debe ser tomado como una previsión de resultados.

- La Universidad Internacional de Andalucía velará en todo momento por preservar el buen uso del perfil y, por ello, la Universidad Internacional de Andalucía, como administrador, se reserva el derecho a eliminar, sin derecho a réplica, cualquier aportación que:

    - Considere ilegal, irrespetuosa, amenazante, infundada, calumniosa, inapropiada, ética o socialmente discriminatoria o laboralmente reprochable o que, de alguna forma, pueda ocasionar daños y perjuicios materiales o morales a la Universidad Internacional de Andalucía, sus empleados, colaboradores o terceros.

    - Incorpore datos de terceros sin su autorización.

    - Contenga cualquier tipo de recomendación relativa a las funciones y competencias de la Universidad Internacional de Andalucía privilegiada o material publicitario o de comunicación, personal o en beneficio de terceros, sean personas físicas o jurídicas.

    - Sea redundante.

    - No esté relacionada con la finalidad perseguida por la Universidad Internacional de Andalucía al darse de alta en la red social de que se trate.

11.3 Uso de medios sociales con fines exclusivamente personales

En ocasiones, el uso personal o profesional de una red social puede llegar a confundirse. Por tanto, se debe ser consciente de las responsabilidades cuando se mezclan la vida personal y la laboral en estos medios.

Las personas que trabajan para la Universidad Internacional de Andalucía deben usar su buen juicio y asumir la responsabilidad personal y profesional de los contenidos que publican a través de los medios sociales.

Es frecuente que se admita el uso de una cuenta personal para comentar sobre asuntos no relacionados con el trabajo, aunque no debiera permitirse, de manera general, que el uso de tales cuentas se lleve a cabo en horario laboral ni, por motivos de seguridad, usando los medios electrónicos de la Universidad Internacional de Andalucía.

En cualquier caso, el uso de plataformas de redes sociales nunca debe interferir con las funciones principales, con la excepción de aquellos puestos de trabajo que incluyan entre sus tareas precisamente el uso de estas herramientas sociales.

Debemos recordar que el uso de una cuenta privada no exime de cumplir los códigos de buena conducta generalmente admitidos y los específicamente contemplados en la Política de Seguridad de la Información de la Universidad Internacional de Andalucía.

Por todo ello, no deben publicarse opiniones personales a través de cuentas oficiales y tampoco promover las cuentas personales a través de cuentas oficiales.

No debe comentarse en redes sociales aquello que no se debe ser de dominio público, aunque exista una única persona a la que se desee dejar al margen. Las redes sociales pueden actuar de amplificador y comprometer a sus usuarios.

Aquellas personas que tienen responsabilidades de gobierno, en virtud de su posición, deben tener en cuenta si los comentarios personales que publican, incluso en lugares claramente personales, pueden ser mal interpretados como declaraciones realizadas por la Universidad Internacional de Andalucía.

11.4 Medidas de seguridad de la información

En primer lugar, es preciso identificar claramente los canales oficiales de la Universidad Internacional de Andalucía que ya pudieran existir y, en la medida de lo posible, diferenciar los canales verdaderos e impulsar la vigilancia y el cierre de canales falsos.

11.5 Medidas de seguridad tecnológica

Las cuentas en redes sociales de la Universidad Internacional de Andalucía se crearán desde correos electrónicos corporativos, delegándose la gestión de las mismas en las unidades organizativas designadas para cada una de ellas.

El Responsable de Seguridad de la Universidad Internacional de Andalucía extenderá sus competencias a los perfiles de redes sociales que pudieran crearse.

La custodia de las contraseñas de los perfiles de las redes o de sus administradores que así lo requieran, estará centralizada y será responsabilidad de la unidad organizativa de la entidad de que se trate.

Cualquier instalación de aplicaciones de terceros que tenga algún tipo de permisos sobre cuentas de las redes sociales deberá ser previamente autorizada por el Responsable de Seguridad de la Universidad Internacional de Andalucía, para verificar que esta aplicación no pone en riesgo ni los datos ni la seguridad de la cuenta.

La modificación de cualquiera de las opciones de privacidad o publicación de comentarios deberá autorizarse previamente por la Universidad Internacional de Andalucía, contando con la opinión del Responsable de Seguridad.

Como norma general, las contraseñas de las plataformas de gestión deberán ser robustas.

Siempre que sea posible, es conveniente mantener las cuentas desde una herramienta de gestión que pueda otorgar permisos diferentes de publicación y que su acceso no se realice a través de la propia contraseña de la red social de que se trate. El responsable de cada cuenta definirá quiénes son las personas que la gestionarán, velando y haciendo respetar la confidencialidad de las contraseñas de acceso.

Siempre que sea posible, el acceso a las cuentas se realizará desde sistemas corporativos. En caso de necesitar publicar contenidos desde un dispositivo móvil, se hará desde una aplicación diferente a la que se utiliza de modo personal.

12 Incidentes de seguridad

12.1 Cuando un usuario detecte cualquier anomalía o incidencia de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de la Universidad Internacional de Andalucía o su imagen, deberá informar inmediatamente a la Comisión de Seguridad. Para ello, se deberá utilizar el sistema de gestión de incidencias de la UNIA, donde quedará registrada y será elevada al área o responsable que corresponda.

13 Compromiso de los usuarios

Es responsabilidad directa del usuario:

13.1 Custodiar las credenciales que se le proporcionen y seguir todas las recomendaciones de seguridad fijadas por la Universidad Internacional de Andalucía, para garantizar que aquellas no puedan ser utilizadas por terceros. Deberá cerrar su cuenta al terminar la sesión o bloquear el equipo cuando lo deje desatendido.

13.2 En el caso de que su equipo contenga información sensible, confidencial o protegida, esta deberá cumplir todos los requisitos legales aplicables y las medidas de protección que la normativa de la Universidad Internacional de Andalucía establezca al respecto.

13.3 Además de lo anterior, no se podrá acceder a los recursos informáticos y telemáticos de la Universidad Internacional de Andalucía para desarrollar actividades que persigano tengan como consecuencia:

- El uso intensivo de recursos de proceso, memoria, almacenamiento o comunicaciones, para usos no profesionales.
- La degradación de los servicios.
- La destrucción o modificación no autorizada de la información, de manera premeditada.
- La violación de la intimidad, del secreto de las comunicaciones y del derechoa la protección de los datos personales.
- El deterioro intencionado del trabajo de otras personas.
- El uso de los sistemas de información para fines ajenos a los de la Universidad Internacional de Andalucía, salvo aquellas excepciones que contempla la presente Normativa.
- Dañar intencionadamente los recursos informáticos de la UniversidadInternacional de Andalucía o de otras instituciones.
- Incurrir en cualquier otra actividad ilícita, del tipo que sea.

14 Monitorización y aplicación de esta normativa

La Universidad Internacional de Andalucía, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente:

- Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
- Monitorizará los accesos a la información contenida en sus sistemas.
- Auditará la seguridad de las credenciales y aplicaciones.
- Monitorizará los servicios de internet, correo electrónico y otras herramientas de colaboración.

La Universidad Internacional de Andalucía llevará a cabo esta actividad de monitorización sin utilizar sistemas o programas que pudieran atentar contra los derechos constitucionales de los usuarios, tales como el derecho a la intimidad personal y al secreto de las comunicaciones, manteniéndose en todo momento la privacidad de la información manejada, salvo que, por requerimiento legal e investigación sobre un uso ilegítimo o ilegal, sea necesario el acceso a dicha información, salvaguardando en todo momento los derechos fundamentales de los usuarios.

Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos temporalmente. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca. El Responsable de Seguridad, con la colaboración de las restantes unidades de la Universidad Internacional de Andalucía, velará por el cumplimiento de la presente Normativa General e informará al Comité de Seguridad sobre los incumplimientos o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa. Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los mismos de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino. Igualmente, el sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar sobre usos prolongados e indebidos del servicio.

15 Incumplimiento de la normativa

Todos los usuarios de la Universidad Internacional de Andalucía están obligados a cumplir lo prescrito en la presente Normativa de Seguridad de la Información.

En el supuesto de que un usuario no observe alguna de los preceptos señalados en la presente Normativa, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos asignados a tal usuario.