Servicio de Informática y Comunicaciones

SIC-PO-001 Normativa de seguridad de la información

universidad de león

	REDACTADO	REVISADO	APROBADO
NOMBRE	Jose Manuel Sáenz de Santa María Fernández	Comité de Seguridad de la Información	
CARGO	VPS CONSULTING S.L.U.		

Fecha de Revisión: 12 de Septiembre de 2023	**Revisión:** 0.4

Tabla de contenido

Manual del Sistema Integrado de Gestión del SIC de la ULE		
Hoja de control de revisiones. Hoja 1 de 1		
Nº Revisión	**Fecha**	**Naturaleza de la revisión**
0.1	25.05.2018	Primer ejemplar
0.2	06.06.2018	Revisión de la normativa por la dirección del SIC
0.3	19.05.2023	Revisión de la normativa por VPS CONSULTING S.L.U.
0.4	12.09.2023	Revisión de la normativa por el Comité de Seguridad de la Información

1. Introducción

Normativa para el establecimiento de la seguridad de la información de la Universidad de León conforme al Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS)

2. Objetivo

Los Sistemas de Información constituyen elementos básicos para el desarrollo de las misiones encomendadas a la Universidad de León, 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 de León 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 de León tiene como objetivo establecer normas encaminadas a alcanzar la mayor eficacia y seguridad en su uso.

3. Alcance

Esta Normativa es de aplicación a todo el ámbito de actuación de la Universidad de León, 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 de León, incluyendo el personal de proveedores externos, cuando sean usuarios de los Sistemas de Información de la Universidad de León.

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

4. Vigencia

La presente Normativa de Seguridad de la Información de la Universidad de León ha sido aprobada por el Rector a propuesta del Comité de Seguridad de la Información, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que la Universidad de León 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 de León.

5. 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 de la Información revisará la presente Normativa, que se someterá, de haber modificaciones, a la aprobación del Rector de la Universidad de León.

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.

6. Utilización del equipamiento informático y de comunicaciones

La Universidad de León 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 de León 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 de León, 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 de León 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.

6.1 Normas generales

- Los ordenadores personales deberán utilizarse únicamente para fines corporativos y como herramienta de apoyo a las competencias profesionales de los usuarios autorizados.
- Se recomienda que 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 de León. Cuando se precise instalar dispositivos no provistos por la Universidad de León deberá solicitarse autorización previa al Servicio de Informática y Comunicaciones.
- 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 Servicio de Informática y Comunicaciones.
- Será responsabilidad de cada Departamento, Servicio o usuario individual el cumplimiento de esta normativa, especialmente en cuanto a las operaciones que haga en cada dispositivo conectado a la red como usuario con privilegios de administración y que atente contra la seguridad de la información alojada en la Universidad de León. El responsable de seguridad verificará el cumplimiento de estas medidas.
- 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 indicará 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 de los programas antivirus y cortafuegos.
- 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 disquetes, CDs/DVDs, memorias USB, mensajes de correo electrónico o instalación de programas descargados desde Internet. Es imprescindible, por tanto, vigilar el uso responsable de los equipos para reducir este riesgo.
- El usuario será responsable de toda la información extraída fuera de la organización a través de dispositivos tales como memorias USB, CDs, DVDs, etc., que le hayan sido asignados. 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 inmediata al Servicio de Informática y Comunicaciones, 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 de León 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.
- El correo facilitado por la Universidad de León es exclusivamente para uso profesional, la Universidad de León se reserva la capacidad previa autorización del Responsable de Seguridad y del propietario de la información, debidamente justificada y por escrito, a recuperar la información necesaria para el correcto funcionamiento de la Universidad.
- Las herramientas colaborativas y de almacenamiento facilitadas por la Universidad de León son exclusivamente para uso profesional, la Universidad de León se reserva la capacidad previa autorización del Responsable de Seguridad y del propietario de la información, debidamente justificada y por escrito, a recuperar la información necesaria para el correcto funcionamiento de la Universidad.

6.2 Recursos de almacenamiento de la Universidad de León

- Respecto al uso de los recursos de almacenamiento facilitados por la universidad de León se tendrán en cuenta las siguientes consideraciones:
    - **Alumno**. Solo podrá utilizar los recursos facilitados por la Universidad de León para uso estrictamente relacionado con la actividad universitaria, el acceso a dichos recursos será deshabilitado al acabar la relación con la Universidad.
    - **PTGAS, PDI y PI** Solo podrá utilizar los recursos para uso estrictamente profesional, el acceso a dichos recursos será deshabilitado al acabar la relación con la Universidad.
- Se considerará que la relación con la Universidad finaliza:
    - En el caso de personal sujeto a contratación, en el plazo de un año, a la finalización del contrato.
    - En el caso de los alumnos, si pasado el plazo de 1 año no ha realizado ninguna matricula o inscripción en cursos facilitados por la Universidad que proporcione acceso a las herramientas de almacenamiento.

- Transcurrido el plazo de 1 año se avisará por correo avisando de que se va a proceder al borrado de la información, con un mes de plazo para que el usuario pueda hacer copia de la información que considere. Esta comunicación se realizará pidiendo confirmación por parte del usuario de que ha recibido el aviso. En el caso de que no se confirme que se ha recibido el aviso se intentará contactar por otros medios.
- Si después de esto no se obtuviera confirmación de que se ha recibido el aviso se procederá a deshabilitar el acceso durante un mes y posteriormente se borrara la información.

6.3 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 de sobremesa, servidor o dispositivo no facilitado por la Universidad de León, sin la previa autorización del Servicio de Informática y Comunicaciones.
- Utilización de conexiones y medios inalámbricos con tecnologías WiFi, Bluetooth o infrarrojos que no estén debidamente autorizados por el Servicio de Informática y Comunicaciones de la Universidad de León.
- Utilización de dispositivos USB, teléfonos móviles u otros elementos, como acceso alternativo a Internet, salvo autorización y solicitud expresa del Servicio de Informática y Comunicaciones.
- 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.

6.4 Normas específicas para el almacenamiento de información

- Con carácter general, la información almacenada de forma local en los ordenadores personales de los usuarios (disco duro local, por ejemplo) no será objeto de salvaguarda mediante ningún procedimiento corporativo de copia de seguridad. Por tanto, cuando tal almacenamiento esté autorizado en las normas internas correspondientes, se recomienda a los usuarios la realización periódica de copias de seguridad, especialmente de la información importante para el desarrollo de su actividad profesional.
- La Universidad de León puede poner a disposición de ciertos usuarios unidades de red compartidas para contener las salvaguardadas periódicas de sus unidades locales. Debe tenerse en cuenta que tales unidades corporativas son un recurso limitado y compartido por todos los usuarios, por lo que sólo deberá salvaguardarse la información que se considere estrictamente necesaria.
- No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento, compartidos o locales, salvo autorización previa del Servicio de Informática y Comunicaciones.

6.5 Normas específicas para equipos portátiles y móviles

- Los teléfonos móviles corporativos serán asignados por el Servicio de Informática y Comunicaciones a petición del Responsable de Área correspondiente.
- Existirá un inventario actualizado de los equipos portátiles y móviles que será gestionado por el Servicio de Gestión Económica y Patrimonio (Inventario).
- 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 Servicio de Informática y Comunicaciones para la adopción de las medidas que correspondan y a efectos de baja en el inventario.
- Los equipos portátiles y móviles deberán utilizarse únicamente para fines institucionales, especialmente cuando se usen fuera de las instalaciones de la Universidad de León.
- Los usuarios de estos equipos se responsabilizarán de que no serán usados por terceras personas ajenas a la Universidad de León 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 de León, 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.).
- Al igual que con el resto de equipos, será responsabilidad de cada Departamento, Servicio o usuario individual el cumplimiento de esta normativa, especialmente en cuanto a las operaciones que haga en cada dispositivo conectado a la red como usuario con privilegios de administración. Será necesario tener en cuenta las medidas de seguridad adecuadas a la sensibilidad de la información manejada y mantener la configuración de seguridad mínima para evitar daños a la información alojada en la Universidad de León. El responsable de seguridad verificará el cumplimiento de estas medidas.

6.6 Uso de memorias/lápices USB (pendrives)

- Se recuerda que las memorias USB están destinadas a un uso exclusivamente profesional, como herramienta de transporte de ficheros, no como herramienta de almacenamiento. La Universidad de León podrá poner a disposición de los usuarios de aplicaciones, servicios y sistemas de la Universidad de León unidades de almacenamiento en red, que podrán usarse para tal propósito.
- Se recomienda el cambio periódico de contraseña de acceso al dispositivo USB. Así mismo es recomendable el establecimiento de controles de acceso a los documentos del dispositivo con permisos de lectura, escritura y ejecución. Sobre dichos documentos se implementarán mecanismos de cifrado de la documentación.
- La pérdida o sustracción de una memoria USB, con datos personales o especialmente protegidos con indicación de su contenido, deberá ponerse en conocimiento del Servicio de Informática y Comunicaciones, de forma inmediata para realizar las acciones oportunas.

6.7 Grabación de CDs y DVDs

- Con carácter general, se recomienda no utilizar equipos grabadores de CDs y DVDs.
- Por razones de seguridad, los equipos nuevos adquiridos por la Universidad de León no dispondrán de grabadores de CDs y DVDs. En el caso de ser necesaria su instalación, deberá justificarse por el usuario y requerirá la previa autorización del Responsable de Area y del Servicio de Informática y Comunicaciones.

6.8 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 de León 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, lo pondrá inmediatamente en conocimiento del Servicio de Informática y Comunicaciones

6.9 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 pondrá inmediatamente en conocimiento del Servicio de Informática y Comunicaciones.

6.10 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.

6.11 Cuidado y protección de la documentación impresa

- 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 y ser custodiada en armarios bajo llave.
- 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 de León de forma que no sea recuperable la información que pudieran contener.
- 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, o crítica para su trabajo.
- Por razones ecológicas y de seguridad, antes de imprimir documentos, el usuario debe asegurarse de que es absolutamente necesario hacerlo.

6.12 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.

6.13 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.

7. Acceso a los sistemas de información y a los datos tratados

- Los usuarios tendrán autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones. El acceso a la información será personal y las credenciales de acceso, intransferibles.
- Cuando un usuario deje de atender un PC durante un cierto tiempo, es necesario bloquear la sesión de usuario o activar el salvapantallas, para evitar que ninguna persona pueda hacer un mal uso de sus credenciales, pudiendo llegar a suplantarlo. Deberá salvaguardar cualquier información, documento, soporte informático, dispositivo de almacenamiento extraíble, etc., que pueda contener información confidencial o protegida frente a posibles revelaciones o robos de terceros no autorizados.

8. 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, o bien un sistema de certificado digital software, para el acceso a los Sistemas de Información de la Universidad de León, 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 sospechas de que sus credenciales están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar al Centro de Atención a Usuarios (CAU) el correspondiente incidente de seguridad.
- Los usuarios deben utilizar contraseñas seguras de acuerdo a las recomendaciones de seguridad de las contraseñas establecidas en la Universidad de León. 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 llamada telefónica solicitándole su nombre de usuario y contraseña, nunca facilitará dichos datos y procederá a comunicar este hecho al Servicio de Informática y Comunicaciones, de forma inmediata.

9. 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 de León 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.

10. Acceso de terceros a los edificios

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

- El personal ajeno a la Universidad de León que temporalmente deba acceder a los Sistemas de Información de la Universidad de León, deberá hacerlo siempre bajo la supervisión de algún miembro acreditado de la Universidad de León (responsable).
- Cualquier incidente que surja antes o en el transcurso del acceso a la Universidad de León deberá ponerlo en conocimiento de su responsable.
- Para los accesos de terceros a los sistemas de información de la Universidad de León, siempre que sea posible, se les crearán usuarios temporales que serán eliminados una vez concluido su trabajo en la Universidad de León. 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 de León.
- Para acceder a los edificios, instalaciones o dependencias de la Universidad de León 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 de León, que constituirá su enlace durante su estancia en él.

- Una vez en el interior de los edificios, dependencias o instalaciones de la Universidad de León, 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 de León.
- 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.

11. Protección de datos de carácter personal y deber de secreto

- La información contenida en las bases de datos de la Universidad de León que comprenda datos de carácter personal está protegida por la normativa vigente, europea y nacional, en materia de Protección de Datos. Los Ficheros o Tratamientos de datos de carácter personal han de adoptar las medidas de seguridad que se correspondan con las exigencias previstas o derivadas de la antedicha normativa.
- Todo usuario de la Universidad de León ó de terceras organizaciones que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la Universidad de León.

12. 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 de León, 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.

12.1 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.
- Se recomienda utilizar las herramientas y programas de correo electrónico suministrados, instalados y configurados por la Universidad de León.
- El correo corporativo deberá utilizarse, única y exclusivamente, para la realización de las funciones encomendadas al personal, evitando el uso privado del mismo.
- Se deberá notificar al Servicio de Informática y Comunicaciones 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 deberá notificar esta circunstancia al Centro de Atención a Usuarios (CAU)
- 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

12.2 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.
- La utilización del correo corporativo como medio de intercambio de ficheros especialmente voluminosos sin autorización, y el envío de información sensible, confidencial o protegida.

13. Acceso a internet y otras herramientas de colaboración

- El acceso corporativo a Internet es un recurso centralizado que la Universidad de León 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 de León 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.

13.1 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.
- Se recomienda acceder a Internet mediante el navegador suministrado y configurado por el Servicio de Informática y Comunicaciones en los puestos de usuario.
- Deberá notificarse al Centro de Atención a Usuarios de la Universidad de León (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.

13.2 Usos específicamente prohibidos

Quedan prohibidas las siguientes actuaciones:

- 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.

14. Incidencias de seguridad

- 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 de León o su imagen, deberá informar inmediatamente al Centro de Atención a Usuarios (CAU), que lo registrará debidamente y elevará, en su caso.

15. Compromiso de los usuarios

Es responsabilidad directa del usuario:

- Custodiar las credenciales que se le proporcionen y seguir todas las recomendaciones de seguridad fijadas por la Universidad de León, 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.
- 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 de León establezca al respecto.

Además de lo anterior, no se podrá acceder a los recursos informáticos y telemáticos de la Universidad de León para desarrollar actividades que persigan o 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 derecho a 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 de León, salvo aquellas excepciones que contempla la presente Normativa.
- Dañar intencionadamente los recursos informáticos de la Universidad de León o de otras instituciones.
- Incurrir en cualquier otra actividad ilícita, del tipo que sea.

16. Monitorización y aplicación de esta normativa

- La Universidad de León, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente:
  a) Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
  b) Monitorizará los accesos a la información contenida en sus sistemas.
  c) Auditará la seguridad de las credenciales y aplicaciones.
  d) Monitorizará los servicios de internet, correo electrónico y otras herramientas de colaboración.
- La Universidad de León 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 ilegitimo 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 de León, 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.

17. Incumplimiento de la normativa

- Todos los usuarios de la Universidad de León 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, y en caso de extrema urgencia y necesidad, el Servicio de Informática y Comunicaciones podrá acordar la suspensión temporal de los recursos electrónicos asignados a tal usuario por un máximo de cuatro semanas. Excedido ese tiempo, el responsable de seguridad podrá acordar la suspensión definitiva.

18. Glosario

- **Seguridad de la Información:** Es la protección de la información y de los sistemas de información frente al acceso, uso, divulgación, alteración, modificación o destrucción no autorizadas, con el fin de proporcionar confidencialidad, integridad y disponibilidad.
- **Medidas de Seguridad:** Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.
- **Guía de Seguridad CCN-STIC-800:** Esquema Nacional de Seguridad. Glosario de términos y abreviaturas. https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/499-ccn-stic-800-glosario-de-terminos-y-abreviaturas-del-ens/file.html