PROTOCOLO DE PROTECCIÓN DE SECRETOS EMPRESARIALES DE LA UNIVERSIDAD DE LEÓN

Aprobado Consejo de Gobierno 19-03-2024

La Directiva (UE) 2016/943 destaca la protección de los conocimientos técnicos y la información empresarial no divulgada, o "secretos empresariales", resguardándolos de su adquisición, uso y divulgación ilícitos. Esta directiva, traspuesta a la legislación nacional con la Ley 1/2019, junto con la Ley de la Ciencia, la Tecnología y la Innovación (LCTI) reconoce que instituciones académicas como la Universidad, al igual que las empresas privadas, invierten significativamente en la creación y aplicación de este capital intelectual. Tal inversión genera ventajas competitivas, impulsando de manera significativa la investigación, la innovación y la transferencia.

Históricamente, se han protegido los resultados de investigación a través de derechos de propiedad industrial e intelectual, como patentes o derechos de autor. Sin embargo, hay conocimiento y resultados generados en el ámbito de la actividad universitaria, que no se protegen adecuadamente con estos métodos tradicionales.

Los "secretos industriales", ahora conocidos como "secretos empresariales", abarcan no solo conocimientos técnicos, sino también datos e información relevante en áreas comerciales, científicas y tecnológicas. Es crucial que estos secretos se integren, al igual que otras formas de propiedad intelectual, en el patrimonio de la Universidad.

Con la tendencia creciente hacia la investigación colaborativa, y más aún en colaboraciones transfronterizas, es vital contar con protocolos para proteger el intercambio de conocimiento entre la universidad y otras entidades.

Dado este panorama y, reconociendo la histórica omisión de aplicar adecuadamente los secretos empresariales en el ámbito universitario, es pertinente introducir este Protocolo de Protección bajo el Secreto Empresarial del Conocimiento e Información Confidencial generados en la Universidad de León. Este protocolo tiene el propósito de establecer un marco claro y coherente que garantice que estos activos sean gestionados y protegidos de manera adecuada en consonancia con las directrices nacionales e internacionales.

1. OBJETIVOS DEL PROTOCOLO

Establecer un procedimiento de actuación del tratamiento del conocimiento y la información confidencial, utilizando para ello la figura jurídica del secreto empresarial en la Universidad de León.

2. ÁMBITO DE APLICACIÓN

El presente Protocolo abarca la Universidad de León, incluyendo a todo el personal que forme parte, ya sea directamente o a través de entidades adscritas o asociadas. Se enfoca particularmente en aquellos involucrados en actividades de investigación, desarrollo e innovación, así como a cualquier persona que, por su relación jurídica con la Universidad, pueda tener acceso a información sensible o confidencial, independientemente de la naturaleza y duración de dicha relación.

Además, se reconoce y engloba a estudiantes, becarios y alumnos en prácticas que, participando en actividades relacionadas con la investigación, tengan o puedan tener acceso a información sensible o confidencial. Este reconocimiento se extiende a quienes, en el contexto de su vinculación con la Universidad, hayan suscrito cláusulas de confidencialidad o, por la naturaleza intrínseca de sus actividades, estén en posición de acceder a dicha información.

En un horizonte más amplio, el Protocolo se hace igualmente extensivo a colaboradores y asociados externos. Se incluye a aquellos que, sin una afiliación directa con la Universidad de León, colaboren en actividades innovadoras, proyectos de investigación, transferencia o en acuerdos de cooperación con terceros. Este abanico cubre a aquellos que, en el marco de colaboraciones o asociaciones con la Universidad o sus entidades adscritas o asociadas, accedan a información de relevancia y significado para la institución.

3.- PRINCIPIOS

1. El conocimiento generado dentro del ámbito propio de la Universidad, en particular en los diferentes proyectos de investigación o procesos de innovación y transferencia, tanto en los que la Universidad participe de manera individual como en colaboración o cooperación con terceros, así como la información relevante que se posea o a la que tenga acceso, que no sea de conocimiento general y que aporte una ventaja a la Universidad o que pueda ser susceptible de generar dicha ventaja, será tratado bajo las normas de este Protocolo.

2. El personal propio que desarrolle su actividad en la Universidad de León, así como en sus entidades adscritas o asociadas, deberá actuar de manera responsable con el conocimiento generado en el seno de la Universidad de León y con aquella información que, por su naturaleza, pueda ser susceptible de tener un carácter reservado o confidencial o ser objeto de un tratamiento reservado o confidencial, actuando de manera reservada con respecto a su contenido, de forma que no la difunda ni la divulgue a terceros sin una autorización expresa de la Universidad.

3. La Universidad de León dispondrá de los medios necesarios para que toda información que, debido a su naturaleza pueda ser relevante para la Universidad de León, o bien que pueda generarse o accederse a ella en un proyecto de investigación o un proceso de innovación, pueda ser objeto de la debida protección mediante la aplicación, si fuera el caso, de las figuras que integran la propiedad industrial o intelectual y entre las que se incluye el secreto empresarial.

4. La Universidad de León, a través del Vicerrectorado con competencias en Investigación y Transferencia a través de la Oficina gestora de actividades de Transferencia de Resultados de Investigación, establecerá los impresos, y procedimientos para la ejecución de este protocolo. De igual manera, dicha Oficina llevará la gestión de los secretos empresariales.

5. La Universidad de León, establecerá medidas para la protección de activos intangibles bajo la opción jurídica de secreto empresarial de la Universidad de

León. Éstas comprenderán medidas informáticas (Anexo II) y físicas (Anexo III) para el cumplimiento y control de versiones, al efecto de implementar las medidas razonables que se fijen para la protección del conocimiento. Una vez que el personal de investigación comunique la obtención de resultados y conocimiento susceptibles de ser protegidos mediante la figura de secreto empresarial, deberá seguir estas medidas de protección para garantizar la condición de secreto.

6. El conocimiento o información protegidos bajo "secreto empresarial" es compatible con otros medios de protección de la propiedad industrial e intelectual tales como patentes, modelos de utilidad, diseños o modelos industriales, marcas, variedades vegetales, y los derechos de autor, y sin perjuicio de la protección conferida por ellos. La Universidad de León, por medio del órgano, entidad u oficina designados por ésta, ofrecerá un soporte o servicio de análisis de dicha compatibilidad, cuando puedan existir dudas sobre la aplicación de unos u otros medios de protección en el ámbito de un proyecto de investigación o proceso de innovación.

7. El secreto empresarial es transmisible, y por tanto son susceptibles de ser parte o conformar un activo intangible transferible de manera conjunta o independiente a otros derechos de propiedad industrial o intelectual dentro de un proceso de transferencia. En similares circunstancias aplicadas a otros derechos de propiedad industrial o intelectual objeto de transferencia, la Universidad de León, por medio del órgano, entidad u oficina designados por ésta, será la encargada de establecer los acuerdos correspondientes y las condiciones en que dicho secreto sea transferible.

8. El titular del "secreto empresarial" será la Universidad de León, aplicándose en tal sentido las normas internas reguladas por la Universidad sobre las invenciones laborales en lo que sea compatible. La Universidad será quien legítimamente ejerza el control sobre el "secreto empresarial", y se extiende frente a cualquier modalidad de obtención, utilización o revelación de la información constitutiva de aquél que resulte ilícita o tenga un origen ilícito con arreglo a lo previsto en la normativa española que regula esta modalidad de propiedad industrial.

9. En lo no dispuesto en este Protocolo será de aplicación con carácter subsidiario las disposiciones de la normativa española y europea aplicable al "secreto empresarial" y en particular, las disposiciones de la Ley 1/2019, de 20 de febrero, de Secretos Empresariales.

4.- DEFINICIÓN DE "SECRETO EMPRESARIAL"

A los efectos de este Protocolo, es susceptible de consideración como "secreto empresarial" a aquella información o conocimiento, incluido el tecnológico, científico, industrial, así como el relativo al campo de las humanidades, el de carácter comercial, organizativo o financiero, que reúna las siguientes condiciones:

a) Ser secreto, en el sentido de que, en su conjunto o en la configuración y reunión precisas de sus componentes, no es generalmente conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesible para ellas;

b) tener un valor para la Universidad de León, ya sea real o potencial, precisamente por ser secreto, confidencial o reservado, y

c) haber sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto

5.- VIOLACIÓN DE "SECRETO EMPRESARIAL"

1. El acceso a secretos empresariales sin consentimiento por la Universidad de León, que sean de su titularidad, se considera ilícito cuando se lleve a cabo mediante:

a) El acceso, apropiación o copia no autorizadas de documentos, objetos, materiales, sustancias, ficheros electrónicos u otros soportes, que contengan el secreto empresarial o a partir de los cuales se pueda deducir; y

b) Cualquier otra actuación que, en las circunstancias del caso, se considere contraria a las prácticas leales, o se realicen con mala fe.

2. La utilización o revelación de un secreto empresarial, así catalogado por la Universidad de León y que sea de su titularidad, se consideran ilícitas cuando, sin el consentimiento expreso de la Universidad, las realice:

- quien haya obtenido el secreto de forma ilícita,
- quien haya incumplido un acuerdo de confidencialidad o cualquier otra obligación de no revelar el secreto empresarial,
- quien haya incumplido una obligación contractual o de cualquier otra índole que limite la utilización del secreto empresarial.

3. La obtención, utilización o revelación de un secreto empresarial titularidad de la Universidad de León, se consideran asimismo ilícitas cuando la persona que las realice, en el momento de hacerlo, sepa o, en las circunstancias del caso, debiera haber sabido que obtenía el secreto directa o indirectamente de quien lo utilizaba o revelaba de forma ilícita según lo dispuesto en el apartado anterior.

4. La revelación de un secreto empresarial titularidad de la Universidad de León, o en su caso la producción, oferta o comercialización de aquellos productos o servicios cuyo diseño, características, funcionamiento, proceso de producción, o comercialización se benefician de manera significativa de un secreto empresarial obtenidos, utilizados o revelados de forma ilícita, constituyen utilizaciones ilícitas del secreto, cuando la persona que las realice sepa o, en las circunstancias del caso, debiera haber sabido que el secreto empresarial que incorporan se había utilizado de forma ilícita, con arreglo a lo dispuesto en este Protocolo.

6.- UNIDADES CON COMPETENCIAS EN MATERIA DE SECRETO EMPRESARIAL

Se establece a la actual Oficina de Transferencia de Resultados de la Investigación (en adelante, OTRI) de la Universidad de León, o en aquella otra denominación específica que pase a estar vigente, como oficina o unidad responsable de la recepción y tramitación de las solicitudes de catalogación de "secreto empresarial".

7.- PROCEDIMIENTO DE CATALOGACIÓN DE "SECRETO EMPRESARIAL"

7.1. Iniciación del procedimiento de solicitud:

El procedimiento se inicia a partir de la comunicación formal de invención o secreto, mediante formulario presentado al efecto en la OTRI, por el personal o investigador que obtenga, posea, ostente o tenga acceso de forma legítima el conocimiento o información relevante sobre la que versará el "secreto empresarial" cuya protección interesa.

En el anexo I de este Protocolo se incluye un formulario/impreso-modelo/ normalizado de solicitud.

Al modelo de solicitud (anexo I) se podrá adjuntar la documentación complementaria que se estime pertinente, dirigida a la OTRI, como oficina o unidad responsable de la recepción y tramitación de la solicitud de "secreto empresarial".

La OTRI realizará un análisis inicial de la solicitud y la documentación complementaria aportada, a partir de la cual podrá:

1. Iniciar la tramitación de la solicitud de "secreto empresarial" según lo previsto en este Protocolo.

2. No admitir a trámite dicha solicitud, por no cumplir con las condiciones exigidas, en cuyo caso solicitará subsanar la documentación, o por resultar evidente que lo planteado no pertenece al ámbito de aplicación de este Protocolo.

La OTRI podrá proponer otros títulos de protección, en previsión de las posibles mejores vías de explotación del resultado, lo que trasladará al investigador, para que puedan aportar la documentación necesaria para la tramitación según ese supuesto.

7.2. Valoración de las solicitudes admitidas a trámite:

En los supuestos en que la solicitud haya sido admitida a trámite, y la OTRI haya considerado procedente iniciar la tramitación de "secreto empresarial", se realizará por dicha oficina un proceso confidencial de recopilación del conocimiento o información relevante objeto de tramitación como "secreto empresarial".

Finalmente, la OTRI elaborará un informe de valoración dirigido a la Comisión de Investigación de la Universidad de León en el que propondrá la incorporación en la catalogación de "secreto empresarial" del resultado al que sea referido.

7.3. Comisión de Investigación y registro.

La Comisión de Investigación de la Universidad de León, tras valorar la documentación aportada desde la OTRI, valorará como favorable o desfavorable la incorporación del resultado al *Registro Oficial de la Propiedad Intelectual, Evidencias y Secretos Empresariales de la Universidad de León* bajo la modalidad de "secreto empresarial". Lo que trasladará a la OTRI para la realización del depósito.

En cualquier caso, la decisión se comunicará al investigador, para poder ser subsanadas las deficiencias encontradas.

Anexo I. Modelo de solicitud
Anexo 2. Medidas de protección informática
Anexo 3. Medidas de protección física.
Anexo 4. Modelo de registro de acceso físico
Anexo 5. Modelo de acuerdo de cotitularidad

ANEXO 1

FORMULARIO DE SOLICITUD DE PROTECCIÓN DE RESULTADO DE INVESTIGACIÓN COMO SECRETO EMPRESARIAL DE LA UNIVERSIDAD DE LEÓN

Este formulario se trata de un documento confidencial de la Universidad de León y no se divulgará ninguna parte de su contenido sin consentimiento previo.

Por favor, cumplimente en su totalidad la solicitud y fírmela. Una vez rellenada la solicitud remita una copia electrónica a la OTRI de la Universidad de León (**otri@unileon.es**)

TÍTULO

DATOS DE CONTACTO			
Nombre y apellidos:			
DNI/Pasaporte:		Nacionalidad:	
Área de conocimiento:			
Departamento:			
Institución/Centro:			
Categoría profesional:			
Teléfono:		Email:	

TIPO DE ACTIVO INTANGIBLE	
¿Qué tipo de intangible es?:	☐ Documento ☐ Invención ☐ Diseño ☐ Procedimiento ☐ Formula ☐ Mejora ☐ Dataset ☐ Características técnico-biológicas ☐ Algoritmo ☐ Informe ☐ Código Fuente ☐ Condiciones de cultivo ☐ Características técnico-biológicas ☐ Cepa ☐ Otro Indicar cuál

Se entiende como **autor/inventor** toda persona que haya realizado una aportación intelectual relevante para el desarrollo de la invención o conocimiento, con independencia de la relación con universidad León.

AUTORES DEL ACTIVO INTANGIBLE						
Nombre y apellidos	DNI	Universidad/Empresa/Instituto	Categoría profesional	Email	% de participación	Firma de conformidad

ORIGEN DEL ACTIVO INTANGIBLE		
¿Es compartida la titularidad del activo?	☐ SI	☐ NO
¿Con que empresa/entidad se debe compartir derechos?		
Aporta plantilla de acuerdo de cotitularidad. (Descargue Plantilla ULE o solicítela en la OTRI)	☐ SI	☐ NO
¿Es un proyecto de investigación?	☐ SI	☐ NO
- Citar el título		
- Citar clave orgánica		
- ¿Subvencionado?	☐ SI	☐ NO
- ¿Por quién está subvencionado?		

DESCRIPCIÓN DEL ACTIVO INTANGIBLE	
Describa el activo de forma que se desprenda qué es, y para qué puede servir. Aquí únicamente, debe realizar un resumen.	
Describa el problema que resuelve	
Describa la novedad	
¿Es un activo con salida comercial?	☐ SI ☐ NO
- Indique las posibles aplicaciones industriales y los sectores productivos a los que va dirigido	
- Estaría interesado en la creación de una spin-off como salida?	☐ SI ☐ NO
El posible mercado comercial es	☐ Nacional ☐ Internacional Indicar que países
Palabras clave relacionadas con el activo	

¿En qué grado de desarrollo está?	☐	**TRL 1**: Principios básicos observados y reportados	Fase de Investigación
	☐	**TRL 2**: Concepto y/o aplicación tecnológica formulada	
	☐	**TRL 3**: Función crítica analítica y experimental y/o prueba de concepto característica	
	☐	**TRL 4**: Validación de componente y/o disposición de los mismos en entorno de laboratorio	
	☐	**TRL 5**: Validación de componente y/o disposición de los mismos en un entorno relevante	Fase de desarrollo
	☐	**TRL 6**: Modelo de sistema o subsistema o demostración de prototipo en un entorno relevante	
	☐	**TRL 7**: Demostración de sistema o prototipo en un entorno real.	Fase de Implementación o innovación
	☐	**TRL 8**: Sistema completo y certificado a través de pruebas y demostraciones.	
	☐	**TRL 9**: Sistema probado con éxito en entorno real	

¿A que ODS corresponde?	☐ Objetivo 1: Poner fin a la POBREZA
	☐ Objetivo 2: HAMBRE Cero
	☐ Objetivo 3: Buena SALUD
	☐ Objetivo 4: EDUCACIÓN de calidad
	☐ Objetivo 5: IGUALDAD de género
	☐ Objetivo 6: AGUA limpia y saneamiento
	☐ Objetivo 7: ENERGÍA asequible y sostenible
	☐ Objetivo 8: TRABAJO decente y crecimiento económico
	☐ Objetivo 9: INDUSTRIA, innovación, infraestructura
	☐ Objetivo 10: Reducir INEQUIDADES
	☐ Objetivo 12: CONSUMO responsable y producción
	☐ Objetivo 13: Acción CLIMÁTICA
	☐ Objetivo 14: Vida MARINA
	☐ Objetivo 15: Vida en la TIERRA
	☐ Objetivo 16: Paz, JUSTICIA e instituciones fuertes
	☐ Objetivo 17: ALIANZAS para los objetivos

¿En qué formato se guardan?	☐ Físico Indicar la ubicación (laboratorio, área, …)
	☐ Digital Indicar el formato del archivo

INFORME SOBRE EL ESTADO DEL ARTE			
PATENTES			
Base de datos de patentes	Patente	Problema técnico que resuelve	Ventaja que aporta con respecto al estado del arte
INVENES			
Espacenet Patent search			
Otras (indicar)			
BIBLIOGRAFÍA CIENTÍFICA			
Medio de publicación	Artículo	Problema técnico que resuelve	Ventaja que aporta con respecto al estado del arte
OTRA DOCUMENTACIÓN RELACIONADA			
Fuente	Tipo de documento	Problema técnico que resuelve	Ventaja que aporta con respecto al estado del arte

I) DECLARACIÓN DEL INVENTOR SOBRE EL PROYECTO, CONTRATO O CONVENIO QUE DA ORIGEN A LA INVENCIÓN Y ESTIMACIÓN DEL COSTE DE SU OBTENCIÓN

1. **La invención es resultado de:**

☐ Un proyecto de investigación (citar título del proyecto, clave orgánica, ámbito territorial y entidad financiadora).

☐ Un contrato de Investigación con (citar la institución o empresa, título del proyecto, nº de referencia y financiación)

☐ TFG, TFM o TESIS

☐ Otros

Notas:

En caso de indicar TFG, TFM, TESIS, o similar, debe incluir necesariamente la totalidad de las referencias a la misma, siendo al menos las siguientes:

- Título de la tesis, tutor, director, estado de la misma, participación en la generación de la invención de cada uno de los inventores, incluyéndose la participación del tutor y director. La participación de cada uno de los inventores debe reflejarse tanto en el % de contribución a la invención, como en el detalle de la parte técnica asociada al desarrollo de la propia invención.
- Tipo de financiación recibida para la generación de la invención, pudiéndose ser JCyL, Ministerio, organismo, empresa…. En el caso de haberse financiado un contrato laboral en la ULE (PIRTU, ART83, etc), indicar sus datos de forma expresa para su correcta identificación.
- Fecha de depósito (pasada o futura), fecha de defensa (pasada o futura), tipo de depósito realizado (si se realizó en condiciones embargo), publicaciones, revistas o artículos relacionados, prensa, concursos, etc.

2. Investigadores participantes y relación mantenida con la ULE durante la generación de la Invención

- Indicar lo que proceda.

- Puede emplear asimismo la siguiente tabla (añada tantas filas como necesite) indicando:

NOMBRE INVENTOR	Vínculo con la ULE durante la generación (1)	Situación actual (2)	Forma en la que se realizó la colaboración con la ULE.

(1) Debe indicarse si, durante la generación de la invención pertenece a alguno de los tipos indicados en el art13 de la Ley de la ciencia o situación que motiva la relación con la ULE.

(2) De no mantener relación con la ULE en la actualidad, indicar la fecha de fin de la relación con la ULE y la situación actual.

3. Exponga de forma resumida de los datos del proyecto que origina los resultados: datos administrativos, descripción de los resultados obtenidos, publicaciones, contribuciones a congresos u otras evidencias de la relevancia científico-técnica de los resultados obtenidos.

4. Estimación del coste de obtención de la patente:

Mediante la determinación de los gastos de experimentación que fueron necesarios en las anualidades previas para la obtención de los resultados descritos. Puede calcularse mediante un % del presupuesto financiable del proyecto que haya permitido la generación de la invención para cada anualidad según corresponda.

- Indicar lo que proceda.

- Puede emplear asimismo la siguiente tabla (añada tantas filas como necesite) indicando:

PROYECTO (1)	Anualidad(2)	% (3)	Explicación o detalle del gasto.

NOTAS:

1. Clave orgánica del proyecto
2. Anualidad. Indíquese para cada anualidad un % en la siguiente columna
3. % empleado en la generación de la invención según el presupuesto financiable que consta en UXXI para dicha clave orgánica y dicha anualidad

II) DECLARACIÓN RESPONSABLE DE LOS AUTORES SOBRE LA NO DIVULGACIÓN DE CUALQUIER INFORMACIÓN O CONOCIMIENTO QUE DAN LUGAR AL ACTIVO INTANGIBLE O DEL MISMO ACTIVO INTANGIBLE

Los abajo firmantes declaran:

1. Que la información o el conocimiento susceptible de proteger bajo la opción jurídica de secreto empresarial:

No es conocida al público en general y no ha sido revelada, ya sea de manera tangible o intangible, en cualquier momento o, de cualquier manera, incluyendo, sin carácter exhaustivo:

(i) Cualquier información científica o técnica, invención, diseño, proceso, procedimiento, fórmula, mejora, tecnología o método, concepto, muestras, informes, datos, know-how, trabajos en curso, dibujos, fotografías, herramientas de desarrollo, especificaciones, programas de ordenador, código fuente, código objeto, organigramas, bases de datos, estrategias de marketing, planes, información o proyecciones financieras, operaciones, estimaciones de ventas, planes de negocio, resultados de actividad relativos a las actividades empresariales pasadas, secretos comerciales; planes para productos o servicios, y listas de clientes o proveedores.

2. **Que se comprometen a no revelar**, en ninguna de las formas anteriormente expuestas ni a través de cualquiera otra forma que pudiera quebrar el legítimo control sobre el secreto empresarial.

3. **Que se comprometen a seguir los protocolos de seguridad informática y física** establecida para el efecto en la Universidad de León.

4. **A comunicar al Vicerrectorado de Investigación**, a través de la OTRI, cualquier conocimiento que tengan de los expuesto en el apartado 1 de esta declaración o incumplimiento del compromiso de no revelar el secreto empresarial, según se indica en el apartado 2.

Lo que hacen constar a los efectos oportunos.

León, a __ de _____ de 20__

Nombre y apellidos	DNI	Universidad/Empresa/Instituto	Categoría profesional	Firma de conformidad

ANEXO II

MEDIDAS DE PROTECCIÓN INFORMÁTICA PARA SECRETOS EMPRESARIALES DE LA UNIVERSIDAD DE LEÓN

Este anexo constituye parte del Protocolo de protección de Secretos Empresariales de la Universidad de León para el establecimiento de las medidas informáticas de la Universidad de León respecto a la Ley 1/2019, 20 de febrero de Secretos Empresariales.

1. ¿DÓNDE ALMACENAR LA INFORMACIÓN?

La información relativa al secreto industrial se almacenará en los equipos de almacenamiento de datos alojados en el CPD del Servicio de Informática y Comunicaciones de la Universidad de León, o en aquellas Cloud públicas que cumplan con el nivel correspondiente del ENS, entre las que se pueden encontrar Google, Azure o AWS.

El personal investigador debe tener una contraseña en la cuenta de usuario de la Universidad de León, de acuerdo con lo indicado en el procedimiento SIC-PE-005-Procedimiento_de_Control_de_Accesos correspondiente a la normativa y procedimientos de seguridad que desarrollan la Política de Seguridad de la Información de la Universidad de León.

1.1. Características del equipo

Los equipos utilizados por el personal investigador, deberán adaptarse a lo indicado en los procedimiento SIC-PE-012-Procedimiento_de_Proteccion_de_equipos y SIC-PE-013-Procedimiento_de_Gestión_Dispositivos_Móviles correspondiente a la normativa y procedimientos de seguridad que desarrollan la Política de Seguridad de la Información de la Universidad de León.

2. ¿CÓMO ACCEDER A LA INFORMACIÓN?

La información sensible estará almacenada en una unidad compartida del servicio de almacenamiento de datos en la Cloud de Google mediante el servicio Google Drive, dicha unidad debe ser creada por el investigador en cuestión y será el que permita o deniegue el acceso a dicha información a terceras personas. Por ello es el administrador de permisos de sus unidades compartidas.
Una vez se concede acceso a cualquier usuario, se ha de firmar un contrato de confidencialidad en el cual se exponga que, si se incumple, se tomarán represalias jurídicas en su contra.

3. POLÍTICA Y NORMATIVA DE SEGURIDAD

Para mayor información sobre la política de seguridad de la Información mirar el documento *POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE LEÓN* (Acuerdo Consejo de Gobierno 14/12/2018), así como el documento SIC-PO-001 Normativa de seguridad de la información)

3.1 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.

3.1.1 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 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 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 el 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 de 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.

3.1.2 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 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.

3.1.3 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.

3.1.4 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.

3.1.5 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.

3.1.6 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.

3.2 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.

3.3 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:

- 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 se deben abrir ni ejecutar 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

3.4 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.

3.5 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.

3.6 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.

3.7 Terceras partes

Cuando la Universidad de León preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Universidad de León utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que

ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

4. CONTROL DE VERSIONES

Google Drive realiza el control de versiones de sus documentos, permitiendo revertir cualquier cambio y conociendo fecha y hora del mismo, de tal forma que si entra un intruso al documento, cualquier cambio se puede revertir y se puede ver quién lo ha editado. De este modo, nos podemos hacer una idea de dónde puede venir la brecha de seguridad.

5. COPIAS DE SEGURIDAD

Para mayor información sobre la política de copias de seguridad del Servicio de Informática y Comunicaciones de la Universidad de León, se recomienda la lectura del documento ”SIC-IT-007 Política de copias de seguridad”, indicado en el procedimiento SIC-PE-015-Procedimiento_de_Proteccion_de_la_informacion correspondiente a la normativa y procedimientos de seguridad que desarrollan la Política de Seguridad de la Información de la Universidad de León.

5.1 Copia de respaldo de información de usuarios

Los usuarios son responsables de la realización de copias de respaldo con la frecuencia definida y siempre que haya cambios significativos en la información que manejan, para lo que utilizarán los sistemas de red que a tal efecto les sean habilitadas.

En ningún caso se deberán almacenar copias de respaldo en el domicilio del usuario o en dependencias de terceros ajenas a los sistemas de información de la ULE si no existe un acuerdo previamente suscrito con el tercero en el que se prevea tal posibilidad y se expliciten las cautelas debidas respecto de la custodia de la información almacenada.

Los responsables de las unidades administrativas de la ULE deberán asegurarse de que la información de los empleados a su cargo se salvaguarda de forma satisfactoria.

5.1.1 Ordenadores portátiles

Todos los usuarios de ordenadores portátiles deberán realizar copias de respaldo de sus datos con la regularidad que se especifique. Para la realización de estas copias de respaldo deberá utilizarse la herramienta que, a tal propósito, se defina a nivel corporativo.

5.1.2 Cifrado de soportes almacenados externamente

Toda la información de copias de respaldo que la ULE almacene fuera de sus dependencias debe estar cifrada, según especifica la Normativa de Seguridad. El procedimiento de envío y recepción de soportes permitirá asegurar que éstos no son extraviados ni han sido manipulados durante su transporte.

5.1.3 Transporte de las Copias de Respaldo

El transporte de las copias de respaldo deberá contar con las adecuadas medidas de seguridad que garanticen la no alteración, robo o destrucción de los datos durante su transporte. El transporte de las copias de respaldo con información sensible se deberá realizar utilizando maletas provistas de mecanismos de apertura operados bajo llave y/o mecanismos de cifrado, y cuyas llaves o claves se encontrarán bajo custodia. La responsabilidad de la destrucción o pérdida de información durante el transporte o almacenamiento recaerá sobre el personal / unidad administrativa / personas jurídicas responsables de su gestión.

5.1.4 Herramientas para la generación de copias de respaldo

El área de Sistemas del SIC contará con un conjunto de herramientas para la generación de copias de respaldo, que le permitirá realizar copias de seguridad de los activos y sistemas de información de la ULE sujetos al ámbito de aplicación del ENS. Estas herramientas de copia se detallan en el registro de herramientas para la generación de copias de respaldo.

5.1.5 Control de copias de seguridad

Se deben etiquetar e identificar los soportes dónde se realizan las copias de seguridad, de manera que se pueda llevar un registro de los soportes sobre los que se ha realizado algún respaldo. Así, en el caso de tener que recuperar una información concreta, agilizaremos el proceso al poder consultar fácilmente en qué soporte se ha almacenado. La hoja de registro deberá incluir los siguientes campos: Identificador de soporte: código que identifica el soporte en el que se ha realizado la copia. Tipo de copia: se indicará si es una copia total, incremental, etc. Fecha y hora: cuándo se llevó a cabo la copia. Lugar de almacenamiento: ubicación física donde se encuentra la copia de seguridad. Personal a cargo de la copia: responsables de la realización y conservación de la copia durante el tiempo que se haya establecido. Esta información se encontrará recogida en el archivo "R1-PE-015 Registros de copias de seguridad".

6. PROTOCOLO DE CONTROL Y LIMITACIÓN DE ACCESOS A LOS SISTEMAS TECNOLÓGICOS PARA EVITAR ACCESOS NO AUTORIZADOS A LA INFORMACIÓN Y/O DOCUMENTACIÓN SECRETA.

Se establecerá de acuerdo a lo indicado en los procedimientos SIC-PE-005-Procedimiento_de_Control_de_Accesos y SIC-PE-012-Procedimiento_de_Proteccion_de_equipos correspondiente a la normativa y procedimientos de seguridad que desarrollan la Política de Seguridad de la Información de la Universidad de León.

7. PROTOCOLO Y ESTABLECIMIENTO DE POLÍTICAS DE UTILIZACIÓN DE LOS SISTEMAS INFORMÁTICOS, INCLUYENDO LA REGULACIÓN DEL PROTOCOLO PARA EL TELETRABAJO.

7.1 Uso de Google Drive

A todo investigador de la Universidad de León que comience un proyecto de investigación que deba estar protegido bajo Secreto Industrial, se le entregará un Manual de Implementación de Protocolo de Secreto Industrial, en el cual se definen todas las directrices que ha de tener en cuenta antes de comenzar a trabajar y durante el proceso de compartir información con otros usuarios implicados.
En este manual se define claramente cómo ha de gestionar los permisos de acceso a la información que comparta; dependiendo de la función de cada persona a la que se le vaya a conceder acceso, podrá editar, comentar o simplemente leer el documento. Sólo el investigador que se designe como "administrador" tendrá la posibilidad de compartir cada documento.
Este investigador propietario de la unidad que gestiona los accesos, debe hacerse cargo de eliminar el acceso a la unidad al personal investigador que abandone la ULE o la investigación en cuestión.
La principal ventaja de utilizar Google Drive es la total seguridad que ofrece respecto a sus múltiples servidores distribuidos por todo el mundo; lo cual hace muy complicado acceder a la información mediante el acceso a instalaciones físicas.
Otra de las ventajas es la facilidad que ofrece este servicio para acceder desde cualquier lugar a la información del investigador. Una vez se hayan tomado las medidas previas de ciberseguridad definidas en el manual de implementación, el investigador contará con un dispositivo seguro y propio para trabajar en este entorno.

7.2 Proceso de autenticación

Cualquier investigador que quiera autorizar un dispositivo para acceder a la información pertinente deberá autenticarse en el servicio de la ULE, con su usuario y contraseña segura. A mayores, debe de iniciar sesión en Google con esta cuenta configurada con el factor de doble autenticación.
Sólo el investigador propietario de la unidad tendrá la posibilidad de borrar documentos, todas las demás personas que tengan acceso no podrán descargar de la nube ni borrar ninguna información. Para ello, el investigador ha de gestionar los accesos según el Manual de Implementación del Protocolo de Seguridad Industrial.
Todos los archivos subidos a Google Drive se encriptan con el cifrado propio que ofrece este servicio.

8. PROTOCOLO DE ACTUACIÓN PARA EL USO DE DISPOSITIVOS MÓVILES, PORTÁTILES Y SOPORTES EXTERNOS (AUTORIZACIÓN DE LOS DISPOSITIVOS QUE TIENEN PERMISO PARA ACCEDER A DICHA INFORMACIÓN Y/O DOCUMENTACIÓN, BORRADO REMOTO, CONTROLES DE ACCESO, ENCRIPTACIÓN, ETC.) Y POLÍTICAS DE TRASLADO DE LA INFORMACIÓN Y DE GESTIÓN DE SOPORTES

Cada es responsable de su cuenta institucional y el uso que realiza con la misma, debiendo cumplir las medidas establecidas por la Universidad de León. Se ha de respetar el almacenamiento de la información en la nube y por ello no almacenar dicha información en medios físicos.

En el apartado referido a la autorización de los dispositivos que tienen permiso para acceder a dicha información y/o documentación, borrado remoto, controles de acceso, encriptación, etc. serán los dispositivos requeridos por el personal investigador, en los que haya registrado su cuenta institucional con el proceso de verificación en dos pasos, y los permisos del personal serán los otorgados por el administrador, siendo responsable del control de permisos de su unidad.

ANEXO III

MEDIDAS DE PROTECCIÓN FÍSICA PARA SECRETOS EMPRESARIALES DE LA UNIVERSIDAD DE LEÓN

Este anexo constituye parte del Protocolo de protección de Secretos Empresariales de la Universidad de León para el establecimiento de las medidas físicas de la Universidad de León respecto a la Ley 1/2019, de 20 de febrero de Secretos Empresariales

1. ESPACIOS

El presente anexo prevé las recomendaciones para el acceso físico a los espacios donde se alojan los equipos informáticos, y dispositivos móviles, así como laboratorios y materiales que guardan información y relación con resultados constitutivos de secreto empresarial y que, por tanto, requieren un acceso restringido.

Con el fin de aplicar homogéneamente la normativa de control de accesos se establece, según características, las siguientes clases de espacios:

- Despachos: Espacios de trabajo del personal de la Universidad de León dotados de los equipos informáticos y dispositivos móviles necesarios para el desarrollo de su actividad profesional.

- Oficinas de Investigación: Espacios de trabajo compartido que cuentan con todo lo necesario para que más de una persona pueda realizar tareas administrativas y profesionales.

- Laboratorios de Investigación: Laboratorios donde se llevan a cabo investigaciones que involucran secretos empresariales.

- Salas de archivo y depósitos: Espacios donde se almacenan documentación, muestras o datos sensibles.

- Salas de prototipado y fabricación: Espacios equipados para la fabricación de prototipos u otros productos.

1.1. Procedimiento de accesos

1.1.1 Acceso a Despachos

Cada investigador o personal de la ULE con despacho propio dentro de las instalaciones de la Universidad de León será responsable del acceso a este y custodiará los equipos informáticos o dispositivos electrónicos que haya dentro con información relevante.

Además del investigador y del personal jerárquico correspondiente de la ULE, tendrán acceso a los despachos el personal autorizado de limpieza y de seguridad.

Cada investigador o personal de la ULE con despacho propio debe asegurarse que:

- Permanezca cerrado cuando no haya nadie trabajando en él.
- Fuera del horario de trabajo sólo accederá al despacho el personal autorizado de limpieza y de seguridad.
- En caso de ausencia temporal, el equipo informático o dispositivo electrónico que se utilice y se mantenga activo estará bloqueado mediante contraseña.

1.1.2 Acceso a oficinas de investigación

Las oficinas de investigación son espacios que deben considerarse sensibles a nivel de seguridad porque pueden disponer de equipos o dispositivos con información catalogable como secreto empresarial. Por ese motivo debe asegurarse que:

- Permanecerán cerrados cuando no haya nadie trabajando en ellos.
- Fuera del horario de trabajo sólo accederán a ellos personal autorizado de limpieza y de seguridad.
- En caso de ausencia temporal, el equipo informático o dispositivo electrónico que se utilice y se mantenga activo estará bloqueado mediante contraseña.

1.1.3 Acceso a laboratorios de investigación

Los laboratorios de investigación son espacios importantes a considerar a nivel de seguridad debido a la naturaleza sensible de los experimentos y la información generada.

Por ese motivo debe asegurarse que:

- Los laboratorios son de acceso restringido y que sólo el personal autorizado tiene acceso mediante llave, clave de acceso, tarjeta, huella o cualquier otro mecanismo de control de acceso.
- Permanecerán cerrados cuando no haya nadie trabajando en ellos.
- Fuera del horario de trabajo sólo accederán a ellos personal autorizado de limpieza y de seguridad.
- Se establezca un proceso para el registro y control de visitantes, asegurándose de que se les proporcione una identificación temporal y se les acompañe mientras se encuentren en el laboratorio.

1.2. Acceso a salas de archivos y depósitos

Las salas de archivos y depósitos son espacios donde se ubican los equipos valiosos y documentos físicos confidenciales, por lo que, son espacios especialmente sensibles a nivel de seguridad. Por ese motivo debe asegurarse que:

- Las salas de archivos y depósitos son de acceso restringido y sólo el personal autorizado tiene acceso mediante llave, clave de acceso, tarjeta, huella o cualquier otro mecanismo de control de acceso.
- Permanecerán cerradas cuando no haya nadie trabajando en ellos.
- Se establezca un proceso de registro de acceso para todo el personal para tener un control y seguimiento del acceso.

1.3. Acceso a salas de prototipado y fabricación

Las salas de prototipado y fabricación son espacios que deben considerarse sensibles a nivel de seguridad porque pueden disponer de equipos, dispositivos u objetos con información catalogable como secreto empresarial. Por ese motivo debe asegurarse que:

- Las salas de prototipado y fabricación son de acceso restringido y que sólo el personal autorizado tiene acceso mediante llave, clave de acceso, llave electrónica o cualquier otro mecanismo de apertura.
- Permanecerán cerrados cuando no haya nadie trabajando en ellos.
- Fuera del horario de trabajo sólo accederán a ellos personal autorizado de limpieza y de seguridad.
- Se establezca un proceso para el registro y control de visitantes, asegurándose de que se les proporcione una identificación temporal y se les acompañe mientras se encuentren en el laboratorio.

2. PROCEDIMIENTO DE ALMACENAMIENTO

Todos los documentos, materiales y dispositivos que contienen información confidencial o catalogada como secreto empresarial deben ser guardados en lugar seguro. Esto puede ser un armario con llave, una caja fuerte o la sala de archivo y depósitos.

Los investigadores o el personal de ULE deben asegurarse que estos lugares de almacenamiento están cerrados cuando no estén en uso.

3. PROCEDIMIENTO DE DESTRUCCIÓN DOCUMENTAL

Los documentos que contienen información confidencial o secretos empresariales no pueden ser desechados sin tratamiento alguno. Estos deben ser destruidos de manera segura para que no puedan ser recuperados. Este proceso debe incluir el uso de trituradoras de papel, incineración o servicios de destrucción documental profesionales.

4. PROCEDIMIENTO DE TRANSPORTE

Cuando sea necesario transportar información confidencial o secretos empresariales, bien entre espacios de la ULE, bien externamente, se debe utilizar métodos seguros de transporte. Estos pueden incluir maletines con cerradura, mensajeros de confianza, envío seguro de documentos o cualquier método de transporte seguro profesional.

5. PROCEDIMIENTO DE AUDITORIAS

Se realizarán auditorías de seguridad regularmente para asegurarse de que las medidas de seguridad física están siendo implementadas adecuadamente y son efectivas. Las auditorías pueden incluir la revisión de los procedimientos de almacenamiento, inspecciones físicas de las áreas de almacenamiento, y pruebas de los sistemas de control de acceso.

ANEXO IV

MODELO DE REGISTRO DE ACCESO AL *Laboratorio/sala/etc*

Fecha	**Hora de entrada**	**Hora de salida**	**Nombre y Apellidos**	**Proyecto en el que participa**	**Firma**

universidad de león

ACUERDO ENTRE LA UNIVERSIDAD DE LEÓN Y _____ PARA LA COTITULARIDAD DE LA INVENCIÓN TITULADA _____

En León, a ….. de …… de 20…

REUNIDOS

De una parte, D./Dña._____, con domicilio a estos efectos en Vicerrectorado de _____, edificio Rectorado, Avda. de la Facultad nº 25, 24004 - León, con D.N.I. Nº_____, en representación de la Universidad de León (en adelante ULE), con CIF. Q2432001B, actuando como Vicerrector de _____ en virtud de la RESOLUCIÓN de 8 de febrero de 2021, del Rector de la Universidad de León, por la que se delegan competencias y atribuciones del Rector en otros órganos unipersonales de gobierno.

Y, de otra parte, D./Dña _____ , actuando en representación _____ (*se he de indicar el nombre de la entidad, el tipo de entidad de que se trata, su CIF, el número de inscripción en el Registro que corresponda y su domicilio a efectos de notificaciones derivadas del Acuerdo*), en calidad de _____ (*señalar el cargo que ostenta*) de esta entidad, y con poder suficiente para la firma del presente Acuerdo, tal y como se desprende de _____ (*indicar el documento en el que consta el apoderamiento suficiente del firmante, y que puede ser un poder notarial, un acuerdo de la Asamblea General u órgano similar de la entidad o una norma en la que se especifique dicho apoderamiento*).

Ambos representantes, reconociéndose mutuamente capacidad jurídica suficiente, suscriben en nombre de las respectivas entidades el presente acuerdo y, al efecto

MANIFIESTAN

Que como resultado del trabajo realizado por los investigadores de la ULE _____ y por los investigadores de _____ se han generado resultados susceptibles de explotación consistentes en

universidad de león

"_____" y a tal efecto acuerdan suscribir el presente Acuerdo de cotitularidad conforme a las siguientes

CLÁUSULAS

Primera. - Que el desarrollo del trabajo conjunto entre la ULE y _____ ha dado lugar a la invención titulada "_____" bajo la cotitularidad de ambas entidades en la siguiente proporción, dividiéndose en idéntica proporción los derechos y obligaciones inherentes a la misma:

- …….. % para la ULE
- …….. % para _____

Segunda. – Las partes acuerdan que la invención será objeto te protección mediante la fórmula jurídica de Secreto Empresarial, y que será realizado un depósito del objeto del secreto, así como de la documentación correspondiente a la autoría y originalidad de éste en el REGISTRO Oficial de la Propiedad Intelectual, Evidencias y Secretos de la ULE.

Caso de ser necesario la tramitación de solicitud en algún otro registro oficial, será acordado de forma expresa por las partes.

Los gastos generales de la tramitación de la solicitud y mantenimiento de los costes de protección serán soportados por ambas entidades en proporción a su titularidad.

La gestión y tramitación de la protección corresponderá a la ULE, en la persona de su representante, por lo que _____ autoriza a la ULE a la realización de los trámites administrativos correspondientes.

Tercera. – De proceder, por necesidades derivadas del tipo de registro, la extensión de la protección a otros países será acordada por escrito por las partes; de no estar interesada alguna de ellas, la otra podrá continuar en su nombre, adquiriendo todos los derechos y obligaciones sobre los resultados en aquellos países que realice por sí misma la solicitud.

Cuarta. - Ambas entidades se informarán mutuamente de las gestiones que se realicen para la explotación de la invención, apoyándose en la gestión y proponiéndose de mutuo acuerdo las condiciones de licencia a la entidad licenciada. Se firmará un contrato con el licenciatario por ambas entidades al efecto.

Quinta. - Los beneficios a que diera lugar la explotación comercial de la invención se repartirán en la proporción a la titularidad de la invención, una vez deducidos los gastos de comercialización. La ULE informará puntualmente a _____ de la gestión y balances económicos referentes a la invención.

A efectos de cualquier comunicación relativa al presente contrato, se establecen las siguientes direcciones:

Universidad de León – Vicerrectorado de Investigación y Transferencia
Avda. de la Facultad de Veterinaria, nº 25 – 24004 - León
Teléfono: 987 29 1637
Correo: vice.investigacion@unileon.es

(B) Contacto…
Dirección
Teléfono:
Correo:

Sexta. - El presente contrato surtirá efectos desde la fecha de su firma y mantendrá su validez en tanto se mantenga en secreto la invención o en tanto se encuentren en vigor los títulos de propiedad intelectual e industrial que puedan haberse acordado, así como los contratos firmados al amparo del presente acuerdo.

Séptima. - Cualquiera de las partes, podrá comunicar expresamente a la otra su renuncia de los derechos y obligaciones derivados del presente acuerdo y, por tanto, la otra parte adquirirá la totalidad de la propiedad de la misma. La parte que adquiere los derechos correrá con los gastos de cambio de titularidad que procedan.

Cualquier renuncia o abandono de los derechos derivados del presente acuerdo se realizará por escrito, con suficiente antelación para que la otra parte pueda ejercer los derechos correspondientes, que en el caso de patentes u otros títulos de propiedad

intelectual o industrial será la fecha última para la toma de decisión que condicionará el mantenimiento del derecho.

En cualquier caso, la entidad renunciante, se asegurará de que todos sus investigadores que consten como inventores en los documentos que correspondieran para los registros en los que se depositara la invención, se comprometen a colaborar para la continuación de la tramitación de los expedientes, facilitando la firma de documentos y la notificación de posibles cambios en su domicilio, manteniéndose localizados en todo momento. La entidad renunciante cumplirá con las obligaciones adquiridas hasta ese momento.

Octava. - La ULE y _____ se comprometen a resolver de manera amistosa cualquier desacuerdo que pueda surgir entre las partes.

En caso de conflicto ambas partes acuerdan el sometimiento a la legislación aplicable y a la jurisdicción competente.

Y en prueba de conformidad, las partes firman el presente Acuerdo por duplicado, en lugar y fecha arriba indicados.

Por la Universidad de León Por _____

EL/LA VICERRECTOR/VICERRECTORA
DE _____
Fdo. D./Dña. _____