Política de seguridad de la información de la UOC

Documento aprobado por el Consejo de Dirección de la UOC el día 20 de diciembre de 2021

Índice

4.3. Responsable de seguridad de la información
4.4. Responsable técnico del servicio de ciberseguridad 7

1. Principios

La seguridad de la información tiene como objetivo reducir, hasta un nivel que resulte aceptable, los riesgos a los cuales está sometida la información, los sistemas y los servicios que apoyan la actividad universitaria. Este nivel aceptable debe responder a una valoración conjunta de la gravedad de las amenazas, los recursos disponibles, el respeto a los derechos individuales y el cumplimiento normativo. Solo los órganos de dirección de la Universitat Oberta de Catalunya (UOC) tienen las competencias necesarias para establecer este nivel, ordenar las actuaciones necesarias en materia de seguridad de la información y habilitar los medios para llevarlas a cabo.

La política de seguridad de la UOC se define basándose en los siguientes principios básicos que deben desarrollarse:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión del personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos.
h) Seguridad por defecto.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tráfico.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de actividad.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
o) Mejora continua del proceso de seguridad.

2. Objeto

El objeto de la política de seguridad es fijar el marco de actuación necesario para proteger los sistemas de información, de amenazas internas y externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los principios básicos de confidencialidad, integridad y disponibilidad de la información.

En este sentido, resulta imprescindible establecer, en la política de seguridad de la información, una organización que garantice la correcta distribución de tareas y responsabilidades.

3. Ámbito de aplicación subjetivo

Esta Política de seguridad hay que aplicarla a toda la información que se genera a consecuencia de las actividades académicas, de investigación, de gestión o de difusión, tanto en la Fundació per a la Universitat Oberta de Catalunya (FUOC) como en el resto de las empresas del grupo (en adelante, "el grupo" o "el grupo empresarial"), así como en los tratamientos de los cuales pueda ser objeto, independientemente de que estos sean manuales o automatizados y de que incluya o no datos de carácter personal, y afecta a todos los miembros de la organización, sin excepciones.

4. Asignación de roles y responsabilidades

A continuación, se detallan los roles y las responsabilidades de cada una de las áreas de la UOC implicadas en la seguridad de la información. Debe especificarse, pues, que el ámbito de actuación de las siguientes áreas va más allá de la fundación, dado que su función abarca la totalidad de las empresas del Grupo.

4.1. Responsable del servicio

La persona responsable de servicio tiene las siguientes funciones:

1. Responsabilizarse de la prestación de servicios basados en sistemas de la información de la universidad.
2. Velar por la seguridad de los activos, en cada dimensión de seguridad, según los criterios marcados por el Comité de Seguridad de la Información de la UOC, con el asesoramiento de la persona responsable de seguridad de la información y de la persona responsable de la tecnología de la información.
3. Garantizar la prestación del servicio en condiciones óptimas de disponibilidad, accesibilidad o interoperabilidad

La función de la persona responsable del servicio de la UOC recae en el gerente de la FUOC, que la tiene delegada en el vicegerente de Operaciones.

4.2. Responsables funcionales de los sistemas de información

Las personas responsables funcionales de los sistemas de información tienen las siguientes funciones en el ámbito de la seguridad de la información:

1. Clasificar la información de la cual son responsables según la criticidad que esta tenga para la compañía en términos de confidencialidad, privacidad, integridad, continuidad, autenticidad, no repudio, trazabilidad e impacto mediático.

2. Determinar la categoría de los sistemas de información utilizando como marco de referencia lo establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, que regula el Esquema Nacional de Seguridad.

3. Tener conocimiento de la normativa general o sectorial aplicable a la información de la cual son responsables, incluida la normativa vigente en materia de protección de datos de carácter personal.

4. Velar por la seguridad de los activos correspondientes al proceso de los cuales son responsables, en cada dimensión de seguridad, confidencialidad, disponibilidad e integridad, según los criterios marcados por el Comité de Seguridad de la Información de la UOC, con el asesoramiento de la persona responsable de seguridad de la información.

5. Determinar el uso, los accesos y los privilegios de los sistemas que están bajo su ámbito de responsabilidad.

6. Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes y para que se cumplan.

7. Colaborar en hacer revisiones y auditorías de seguridad de la información.

La función de las personas responsables funcionales de los sistemas de información de la UOC la desarrollan las personas responsables de proceso definidas en el Mapa de procesos del sistema de gestión interna de calidad de la UOC.

4.3. Responsable de seguridad de la información

La persona responsable de seguridad tiene la obligación de velar por la seguridad de la información y de los servicios prestados por los sistemas de información, y dirigir el

sistema de gestión de la seguridad de la información de acuerdo con lo que se establece en esta política. Tiene las siguientes funciones:

1. Elaborar, promover y mantener una política de seguridad de la información.
2. Desarrollar, con el apoyo de las unidades correspondientes, el marco normativo de seguridad y controlar su cumplimiento.
3. Fijar objetivos de seguridad y planificar la ejecución.
4. Planificar las auditorías necesarias para garantizar el cumplimiento de la legalidad vigente y el ciclo de vida del sistema de gestión de la seguridad de la información.
5. Analizar los riesgos que afronta la UOC en el marco de seguridad de la información y tomar decisiones sobre la forma de tratarlos.
6. Es responsable de la elaboración y seguimiento del Plan de seguridad.
7. Promover la adecuación a las normativas.
8. Velar por que se establezcan los mecanismos de continuidad de las actividades ante incidentes de seguridad.
9. Hacer seguimiento de las incidencias de seguridad y escalarlas al Comité de Seguridad si corresponde.
10. Supervisar la eficacia de las medidas de seguridad establecidas para proteger la información y garantizar la disponibilidad y el correcto funcionamiento de los servicios prestados por los sistemas de información.
11. Proponer la implantación de herramientas y controles de seguridad de la información y definir el cuadro de mando de la seguridad.
12. Promover la formación y concienciación de los trabajadores y trabajadoras de la UOC en la seguridad de la información dentro de su ámbito de responsabilidad.
13. Ser el interlocutor o interlocutora oficial en comunicaciones con otras entidades en esta materia.

La función de responsable de seguridad de la información la ejerce la persona que tiene asignada la responsabilidad de dirección de la Oficina de Seguridad de la Información.

4.4. Responsable técnico del servicio de ciberseguridad

La persona responsable del servicio de ciberseguridad tiene las siguientes funciones:

1. Dirigir y coordinar el servicio de operación de la seguridad que monitoriza, levanta alertas e investiga posibles incidentes de seguridad.
2. Coordinar las actividades relacionadas con la detección, el análisis y la gestión de vulnerabilidades.
3. Estar alerta de los cambios de la tecnología de que dispone la UOC y de las consecuencias de estos cambios, y proponer las medidas oportunas.
4. Informar y rendir cuentas a la persona responsable de seguridad de la información en materia de seguridad de la información.

5. Redactar los procedimientos de actuación en el uso de los servicios tecnologías de la información y la comunicación (TIC) relacionados con la seguridad.
6. Coordinar la elaboración de informes técnicos en caso de incidencias de seguridad muy graves.
7. Responsabilizarse de la ejecución regular de verificaciones de seguridad y, si fuera necesario, proponer medidas correctoras.
8. Colaborar en la elaboración y el seguimiento del Plan de seguridad.
9. Elaborar los requisitos de formación y calificación de administradores, operadores y usuarios, junto con la persona responsable del sistema.
10. Identificar las tareas de administración y operación que garanticen la satisfacción de los criterios y requisitos de segregación de tareas impuestas por el Comité de Seguridad de la Información.
11. Responsabilizarse de coordinar la respuesta ante incidentes de seguridad que desborden los casos previstos y procedimentados, y de coordinar la investigación forense relacionada con incidentes considerados relevantes.

La función de responsable técnico del servicio de ciberseguridad la ejerce la persona dentro de la Oficina de Seguridad de la Información designada por la persona responsable de seguridad.

4.5. Responsable del sistema

La persona responsable del sistema tiene las siguientes funciones en relación con la seguridad de la información:

1. Garantizar el desarrollo, la operación y el mantenimiento del sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
2. Aplicar la política de seguridad correspondiente a la conexión o desconexión de equipos.
3. Asegurar la aprobación de los cambios que afecten la seguridad del sistema.
4. Garantizar la implantación de las medidas específicas de seguridad del sistema y asegurarse de que estas se integren adecuadamente dentro del marco general de seguridad.
5. Velar por la implantación de la configuración autorizada de hardware y software para utilizar en el sistema.
6. Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el sistema.
7. Velar por el cumplimiento de las obligaciones en materia de seguridad de cada entidad involucrada en el mantenimiento, operación, explotación, implantación y supervisión del sistema.
8. Dotar los recursos necesarios para investigar los incidentes de seguridad que afectan el sistema y, en su caso, comunicación a la persona responsable de seguridad de la información o a quién esta determine.

9. Establecer planes de contingencia y emergencia según las directrices establecidas en los planes de continuidad, y llevar a cabo ejercicios frecuentes para que el personal se familiarice con estos.
10. Velar por que los proyectos TIC incorporen los principios de protección de datos y de seguridad de la información en el diseño y por defecto.

Además, la persona responsable del sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informada de deficiencias graves de seguridad que puedan afectar la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con las personas responsables de la información afectada y del servicio afectado, así como con la persona responsable de seguridad de la información, antes de ser ejecutada.

La función de responsable del sistema la ejerce la persona que tiene asignada la responsabilidad de dirección de la tecnología de la información en la UOC, es decir, el director o directora del Área de Tecnología.

4.6. Plantilla de la UOC

Las personas que trabajan en la UOC, personal empleado y personal eventual que utiliza los sistemas y aplicaciones de la UOC, tienen las siguientes funciones en el ámbito de la seguridad de la información:

1. Responsabilizarse del correcto tratamiento de los datos personales dentro de su ámbito de actividad.
2. Relacionarse con las TIC para cumplir sus obligaciones laborales.
3. Concienciarse en la seguridad de las TIC para el mantenimiento de la seguridad del sistema.
4. Estar informadas de sus obligaciones y responsabilidades y haber sido correctamente instruidas por las tareas que realizan. Al efecto tendrán a su disposición las normas de uso de los medios tecnológicos y de la información y recibirán la formación adecuada en cada momento, atendiendo a sus responsabilidades.
5. Ser responsables de conocer los procedimientos de su competencia.
6. Ser responsables de informar de cualquier incidente de seguridad que sea observado durante la realización de su actividad laboral diaria.

5. Organización de la seguridad

La UOC dispondrá de una estructura de supervisión y coordinación de la seguridad que será la responsable de establecer y aprobar los requisitos de seguridad para el sistema, además de verificar y supervisar la correcta implementación y mantenimiento de estos requisitos. Esta estructura está formada por los siguientes órganos:

5.1. Consejo de Dirección de la universidad

Funciones:

- Ser el responsable de que la UOC consiga sus objetivos de seguridad TIC a corto, medio y largo plazo.
- Apoyar explícitamente y con notoriedad de las actividades de seguridad TIC a la UOC.
- Expresar sus inquietudes en cuanto a la seguridad de la información al Comité de Seguridad de la Información.
- Aprobar la Política de seguridad de la UOC.
- Delegar el seguimiento de la seguridad en el Comité de Seguridad de la Información.

5.2. Comité de Seguridad de la Información

Funciones:

- Revisar la política de seguridad de la información y propone que el Consejo de Dirección la apruebe.
- Aprobar las normativas asociadas a la política de seguridad de la información.
- Divulgar la política y las normativas de seguridad de la UOC.
- Aprobar del Plan director de seguridad.
- Velar por obtener los recursos necesarios para la consecución de los niveles de seguridad establecidos.
- Seguir periódicamente (dos veces al año) los objetivos de seguridad marcados por el año en curso.

El Comité de Seguridad se reunirá de manera ordinaria dos veces al año, una el primer semestre y una el segundo, y, de manera extraordinaria, tantas veces como sea necesario, a instancia de su presidente o presidenta o de la persona responsable de seguridad de la información.

Formarán parte de este comité las siguientes figuras/personas:

Presidente o presidenta: director o directora general de la FUOC y gerente o gerenta de la universidad.

Secretario o secretaria: persona responsable de la seguridad de la información.

Miembros:

- Director o directora general de la FUOC y gerente o gerenta de la universidad
- Vicerrector o vicerrectora de Docencia y Aprendizaje
- Vicerrector o vicerrectora de Planificación Estratégica e Investigación
- Vicegerente o vicegerenta de Finanzas y Recursos
- Vicegerente o vicegerenta de Operaciones
- Secretario o secretaria general
- Director o directora del Área de Tecnología

- Responsable de la seguridad de la información
- Director o directora de la Asesoría Jurídica
- Delegado o delegada de protección de datos

6. Desarrollo

6.1. Dimensiones de la seguridad

La UOC depende de los sistemas TIC para lograr sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para proteger frente a daños accidentales o deliberados que puedan afectar la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la confidencialidad, disponibilidad e integridad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza en los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, hace falta una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Las diferentes áreas y estudios de la UOC deben asegurarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde la concepción hasta la retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas y en pliegos de licitación para proyectos de TIC.

Las áreas y los estudios de la UOC deben estar preparados para prevenir accidentes, detectarlos, reaccionar y recuperarse.

6.1.1. Prevención

Las áreas y los estudios de la UOC deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Por eso los departamentos deben implementar las medidas de seguridad

adecuadas, así como cualquier control adicional identificado por medio de una evaluación de amenazas y riesgos que se considere adecuado. Estos controles, y los roles y las responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.
Para garantizar el cumplimiento de la política deben:

- Autorizar expresamente la corrección de los sistemas y su configuración, y hay que presentar unos controles de seguridad adecuados antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración, que afecten la seguridad, realizados de forma rutinaria.
- Pedir la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

6.1.2. Detección

Dado que los servicios pueden degradarse rápidamente a causa de incidentes, que van desde una simple desaceleración hasta su detención, deben establecerse medidas para monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

La monitorización es especialmente relevante cuando se establecen líneas de defensa en la seguridad del sistema en estudio. Se establecerán mecanismos de detección, análisis e informe que lleguen a las personas responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

6.1.3. Respuesta

Los departamentos de la UOC deben:

- Establecer mecanismos para responder eficazmente en los incidentes de seguridad (bien directamente o bien mediante entidades centradas en esta respuesta a incidentes).
- Designar un punto de contacto para las comunicaciones en cuanto a incidentes detectados en otros departamentos o en otros organismos que puedan tener impacto.
- Establecer protocolos para el intercambio de información relacionada con el incidente con las entidades que puedan participar en actividades de apoyo y asistencia.

6.1.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, los departamentos de la UOC deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

Un plan de continuidad del negocio tiene que permitir:

- Mantener el nivel de servicio dentro de los límites definidos.
- Minimizar el periodo de recuperación.
- Recuperar la situación inicial previa a un incidente.
- Analizar los resultados y los motivos de los incidentes.
- Minimizar el impacto de un incidente en la actividad de la organización.

En caso de que los incidentes de seguridad hayan podido tener impacto en los servicios o los activos de la organización, habrá que determinar en el plan de continuidad las actuaciones y los protocolos que hay que seguir para permitir la recuperación y continuación de los servicios implicados.

6.2. Principios de la seguridad de la información

El sistema de gestión de la seguridad de la información es el instrumento del cual se dota la UOC para garantizar la integridad, confidencialidad y disponibilidad de la información que trata, así como para garantizar la trazabilidad de las acciones que se llevan a cabo sobre esta. Este sistema debe estar sometido a monitorización, control y mejora continua para mantener la eficacia ante la constante evolución de las amenazas y de los sistemas técnicos de protección.

El sistema de gestión de la seguridad de la información está constituido por un conjunto de documentos (protocolos, normativas y procedimientos), que desarrollan los principios que tienen que regir la aplicación de esta política.

6.2.1. Gestión de riesgos

El análisis y la gestión de riesgos son partes esenciales del proceso de seguridad y deben mantenerse permanentemente actualizados. La gestión de riesgos tiene que permitir el mantenimiento de un entorno controlado, que minimice los riesgos hasta niveles aceptables y que involucre los órganos de dirección de la UOC en la aceptación de un determinado riesgo residual.

El análisis y la gestión de riesgos se tiene que hacer conforme a herramientas y metodologías habitualmente aceptadas y deben estar presentes en todas las fases del ciclo de vida de las aplicaciones y de los servicios y sistemas que apoyan el tratamiento de la información. La selección y la aplicación de los controles de seguridad, así como la evaluación de su eficacia, deben tenerse en cuenta durante el diseño, la construcción, la contratación, la adquisición, la explotación y la terminación o cancelación de las aplicaciones, los servicios y los sistemas mencionados.

La persona responsable de la seguridad de la información debe elaborar un informe anual sobre el estado de la seguridad, los riesgos previsibles y los planes de actuación

recomendados.

6.2.2. Clasificación de la información

Los activos de información que se tratan deben estar inventariados y clasificados. Esta clasificación se debe hacer teniendo en cuenta requerimientos legales, su valor, su sensibilidad y su criticidad por la organización. El nivel de protección y las medidas de seguridad que tienen que aplicarse a la información deben basarse en su clasificación.

6.2.3. Planificación y coordinación

Periódicamente la UOC tiene que definir un conjunto de objetivos de seguridad, que deben incluir una descripción de las líneas de actuación previstas, los proyectos en que se concretan, los objetivos que deben lograrse y los indicadores de cumplimiento y progreso correspondientes. Estos objetivos tienen que tomar en consideración los resultados de las auditorías y del análisis de riesgos.

El esquema organizativo de la seguridad de la información incluye los órganos de coordinación y decisión necesarios para la aplicación y el control de las medidas de seguridad.

6.2.4. Acceso a la información

Las personas que tratan información de la UOC que no tenga carácter público deben estar debidamente acreditadas por unas credenciales electrónicas personales e intransferibles.

Los privilegios de acceso a la información deben limitarse a los estrictamente imprescindibles para el desarrollo de las funciones de cada uno.

6.2.5. Registro de actividad

Las actuaciones de las personas, como forman parte de tratamientos de información, deben grabarse a aplicación de las exigencias legales de trazabilidad o para verificar el cumplimiento de esta política.

6.2.6. Confidencialidad y deber de secreto

Las personas que tratan información de la UOC que no tenga carácter público deben guardar, por un tiempo indefinido, la máxima reserva y no divulgar ni utilizar directamente ni intermediando terceras personas o empresas los datos, los documentos, las metodologías, las contraseñas, los análisis, los programas y otra información a la cual tengan acceso durante su relación laboral con la FUOC y con empresas que pertenecen al Grupo, tanto en soporte material como electrónico. Esta obligación continuará vigente una vez extinguido el contrato laboral.
En el caso de la actividad de investigación, los datos tratados podrán divulgarse convenientemente anonimizados.

6.2.7. Instalaciones y equipamiento

Las infraestructuras informáticas y de comunicaciones que no forman parte de los puestos de trabajo deben ubicarse en áreas aisladas, de acceso restringido y suficientemente protegidas.

6.2.8. Protección de la información no automatizada

La información en soporte no electrónico debe protegerse con el mismo nivel de seguridad que la que haya sido sometida a tratamiento automatizado.

7. Directrices de seguridad de la información

- **Salvaguardia de intereses**, entendida como que cualquier acción o medida implementada en materia de seguridad de la información debe salvaguardar los intereses de la comunidad UOC (estudiantado, profesorado, personal investigador y trabajadoras y trabajadores) y debe permitir el cumplimiento de sus obligaciones.
- **Proporcionalidad y gestión del riesgo**, entendidos como que hay que aplicar medidas de protección de la información para garantizar la disponibilidad, confidencialidad, privacidad e integridad según el principio de proporcionalidad, de forma que las medidas adoptadas para proteger la información sean fruto de un análisis del riesgo existente y del impacto por parte de la UOC en caso de que este riesgo se materializara.
- **Asunción de riesgos**, entendida como que la asunción de riesgos en materia de seguridad de la información tiene que ser aprobada por un nivel directivo adecuado, que será más alto según mayor sea el impacto máximo del riesgo. Este nivel directivo de riesgo debe tener competencia sobre el ámbito afectado en caso de materialización del riesgo.
- **Continuidad del negocio**, entendida como que hay que desarrollar planes de continuidad del negocio de acuerdo con el resultado de un análisis del riesgo para asegurar la continuidad de los procesos críticos.
- **Propiedad y clasificación de la información**, entendidas como que toda información debe tener una persona propietaria responsable de clasificarla en función de su valor y los requerimientos legales existentes, controlar su ciclo de vida y autorizar el acceso a ella.
- **Acceso de acuerdo con el principio de necesidad**, entendido como que solo se facilita acceso a la información a las personas que tengan una necesidad legítima para el desarrollo de sus funciones.
- **Responsabilidad y calidad**, entendidas como que la información proporcionada a través de medios electrónicos debe estar protegida adecuadamente para garantizar su veracidad y autenticidad.

- **Cumplimiento normativo**, entendido como que hay que dar cumplimiento a la legislación y al marco normativo de referencia vigente en materia de seguridad de la información.
- **Relación con terceros**, entendida como que hay que adoptar las medidas necesarias para garantizar la seguridad de la información en la relación con terceras partes. En concreto, los contratos incluirán cláusulas que obliguen a la empresa contratista y, en su caso, subcontratada a aplicar las medidas de seguridad de la información que correspondan en aplicación de esta política, a cumplir o desarrollar los procedimientos de seguridad de la información necesarios y a cumplir otras políticas de la UOC que puedan ser aplicables a la empresa, el servicio o el personal externo que presta el servicio. El contrato debe recoger la posibilidad de realizar auditorías por parte de la UOC, y de penalizar el prestamista de servicios en caso de incumplimiento.
- **Divulgación**, entendida como que se llevarán a cabo acciones de formación y concienciación de todos los usuarios y usuarias en materia de seguridad de la información, y de comunicación de responsabilidades, obligaciones y pautas de comportamiento ético, así como de los procedimientos establecidos por la notificación de incidencias.
- **Uso legítimo**, entendido como que hay que asegurarse de que todos los activos de información, sean alquilados, cedidos, compartidos o propiedad de la UOC, sean para el uso exclusivo en las actividades y los objetivos previstos y legítimos de la UOC, y que no se permita ningún uso privado o para cualquier otro objetivo.
- **Disponibilidad de recursos**, entendida como que se establecerá la estructura de gestión y se asignarán los recursos necesarios para garantizar y controlar la correcta implantación de la seguridad de la información.
- **Segregación de funciones**, entendida como que la asignación de funciones y responsabilidades se hará respetando siempre que sea posible el principio de segregación de funciones (las operaciones de alto riesgo no deberían poder ser realizadas de principio a fin por una sola persona).
- **Seguimiento continuado**, entendido como que se hará un seguimiento continuado del sistema de gestión de la seguridad de la información y de los indicadores que se deriven de este, y se realizarán auditorías regulares de los sistemas para garantizar la aplicación de los controles y medidas de seguridad de la información establecidos, y detectar posibles vulnerabilidades o carencias.

8. Desarrollo de la política de seguridad de la información

La política de seguridad se desarrollará mediante normas, procedimientos, guías y documentos de apoyo de seguridad por cada especificidad.

Estos recursos irán actualizándose periódicamente y se divulgarán y comunicarán tal como se explica en el punto 10 del presente documento.

9. Revisión o control de cumplimiento

La persona responsable de seguridad de la información realizará revisiones o controles periódicos de verificación de la aplicación y el cumplimiento de la política de seguridad, así como del marco normativo que la desarrolla. Desde el Comité de Seguridad se realizarán controles de cumplimiento de la política de seguridad, y también se identificará y se mantendrá actualizada la relación de requisitos legales, organizativos y técnicos que le sean aplicables en materia de seguridad de la información.

Estas revisiones tendrán carácter anual o se llevarán a cabo cuando se produzcan cambios significativos de la política de seguridad o del marco normativo.

10. Divulgación y comunicación

Una vez aprobada la presente política de seguridad, así como la normativa que la complemente, se pondrá a disposición de todos los sujetos afectados por esta según el ámbito de aplicación. Así mismo, los documentos mencionados estarán disponibles en la intranet de la UOC. Para difundir y dar a conocer la política de seguridad y la normativa complementaria, se realizarán píldoras de formación. La asistencia a las sesiones de formación es de carácter obligatorio.
En los contratos, licencias y acuerdos subscritos con terceros por parte de la FUOC se incluirá el deber de cumplimiento de la legislación vigente en materia de seguridad, así como la legislación aplicable en materia de propiedad intelectual y de protección de datos y cualquier otra normativa aplicable. Se informará a los diferentes proveedores, en el momento de la contratación, de la existencia de la política de seguridad a la cual restan sujetos.

11. Aprobación de la política

La aprobación de la presente política se ha llevado a cabo de conformidad con lo previsto en la Política de roles y responsabilidades en la aprobación de normativa interna de la UOC.

12. Confidencialidad

Todas las normas, los procedimientos y los documentos aprobados internamente serán propiedad de la UOC y no podrán utilizarse con fines distintos a aquellos para los que se han entregado ni podrán transmitirse o comunicarse a personas ajenas a los intereses de la UOC.

Firma,

Anexo 1. Marco legal y normativo

Para cumplir con las obligaciones relativas a la seguridad de la información, el marco legal y estratégico de la presente política está formado principalmente por las siguientes directivas, leyes orgánicas, leyes, reales decretos, pactos y normativas internas:

- Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.
- Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.
- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el cual se aprueba el texto refundido de la Ley de Propiedad Intelectual.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Así como el resto de normativa aplicable en la UOC en materia de seguridad de la información.

Anexo 2. Cuadro de versiones

Versión	Fecha	Cambio	Motivo del cambio
1	30/06/2016	Creación.	
2	01/07/2021	La totalidad de la política.	Adecuación a la nueva realidad de la institución y al marco legal vigente.
3	21/01/2022	Cambio en el apartado 5.2.	Cambio en la composición del Comité.