

POLÍTICA DE USO DEL SISTEMA DE INFORMACIÓN

Normas de uso del conjunto de tratamientos, programas, soportes y equipos empleados para el tratamiento de datos de carácter personal y otras informaciones protegidas por el deber de secreto responsabilidad de ESCUELA EUROPEA DE ALICANTE

1. Objetivo del documento

El 4 de mayo de 2016, se publicó en el Diario Oficial de la Unión Europea el 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 (Reglamento general de protección de datos) (DOUE L 119/1, 04-05-2016), en adelante RGPD.

Así mismo, la Agencia Española de Protección de Datos plasmó, en su Plan Estratégico 2015-2019, su voluntad de que los responsables del tratamiento alcancen un elevado cumplimiento de las obligaciones que la normativa de protección de datos les impone, fomentando una cultura de la protección de datos que suponga una clara mejora de la competitividad, compatible con el desarrollo económico.

En este sentido, el Considerando 39 del Reglamento europeo señala que “los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento”.

A este respecto, el artículo 5 del Reglamento (UE) 2016/679, bajo la rúbrica “Principios relativos al tratamiento”, establece que los datos personales deberán ser “tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)” (art. 5.1 f RGPD). Así mismo, el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en dicho apartado y deberá ser capaz de demostrarlo («responsabilidad proactiva») (art. 5.4 RGPD).

En consecuencia, la Dirección / Órgano de Gobierno de **ESCUELA EUROPEA DE ALICANTE** apuesta por una política proactiva de cumplimiento en pos de conseguir que en el desarrollo de sus fines se respete de forma activa el derecho fundamental a la protección de datos.

Firma del usuario del sistema de información:

Nombre y Apellidos:

Fecha:

De tal modo, el artículo 32 del Reglamento (UE) 2016/679, bajo el epígrafe “Seguridad del tratamiento”, establece lo siguiente:

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Así, ex art. 32.4 RGPD, el responsable del tratamiento deberá tomar las medidas para garantizar que cualquier persona que actúe bajo su autoridad y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo las instrucciones del responsable.

Como corolario de todo lo anterior, el presente documento se elabora con el objeto de establecer la Política de uso del sistema de información de **ESCUELA EUROPEA DE ALICANTE**, con la finalidad de dar cumplimiento con lo establecido en los artículos 5.1 f) y 32.1 y 32.4 del Reglamento (UE) 2016/679.

2. Ámbito de aplicación

Las normas contenidas en la presente Política de Uso serán de aplicación a todos los usuarios del sistema de información responsabilidad de **ESCUELA EUROPEA DE ALICANTE**, entendiéndose por tal el conjunto de tratamientos, programas, soportes y equipos empleados para el tratamiento de datos de carácter personal y otras informaciones protegidas por el deber de secreto.

3. Confidencialidad y secreto

El usuario del sistema de información responsabilidad de **ESCUELA EUROPEA DE ALICANTE** debe guardar la debida confidencialidad sobre los hechos, informaciones, conocimientos, documentos, objetos y cualesquiera otros elementos protegidos por el secreto, a los que tenga acceso con motivo de la relación con el responsable del tratamiento.

Firma del usuario del sistema de información:

Nombre y Apellidos:

Fecha:

En tal sentido, y sin carácter limitativo o excluyente, el citado deber de confidencialidad y secreto comprende la siguiente información:

1. Cualquier información sobre personas físicas identificadas o identificables, protegida por la normativa sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales.
2. Cualquier información protegida por la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
3. Cualquier información sujeta al deber de secreto profesional.
4. Cualquier información protegida por la normativa sobre propiedad intelectual e industrial.
5. Los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales).
6. Cualquier otra información que por su naturaleza no pueda ser revelada a terceros ajenos al responsable del tratamiento y que, por lo tanto, no sea de conocimiento público.

El cumplimiento de dicha obligación subsistirá aun después de finalizar la relación con la **ESCUELA EUROPEA DE ALICANTE**.

4. Instrucciones del responsable del tratamiento

El usuario del sistema de información debe cumplir con las normas de seguridad que afecten al desarrollo de sus funciones en el marco de la relación con el responsable del tratamiento, que asimismo son de obligado cumplimiento para las personas con acceso al conjunto de tratamientos, programas, soportes y equipos empleados para el tratamiento de datos de carácter personal y otras informaciones protegidas por el deber de secreto responsabilidad de **ESCUELA EUROPEA DE ALICANTE**.

Asimismo, debe usar los datos de carácter personal responsabilidad de **ESCUELA EUROPEA DE ALICANTE** exclusivamente con las finalidades determinadas, explícitas y legítimas, necesarias para el desarrollo de sus funciones en la citada entidad, para las cuales haya sido autorizado en el marco de la relación con la misma.

De igual manera, se le informa de la prohibición de acceder a los datos de carácter personal responsabilidad de **ESCUELA EUROPEA DE ALICANTE** que no sean precisos para el desarrollo de sus funciones en el marco de la relación con la citada entidad, sin autorización expresa de la misma.

El cumplimiento de dichas obligaciones subsistirá aun después de finalizar la relación con **ESCUELA EUROPEA DE ALICANTE**.

Firma del usuario del sistema de información:

Nombre y Apellidos:

Fecha:

Para el uso de los sistemas informáticos de la Escuela, cada usuario dispone de sus propias credenciales, pertenecientes a los siguientes dominios:

- EscuelaEuropea.org. El usuario y contraseña se generan en la Escuela Europea de Alicante y son almacenados en los servidores del centro. La responsabilidad de las cuentas corresponde al departamento ICT.
- EURSC.org. Credenciales para uso de los ordenadores de la red Administrativa. La responsabilidad de las cuentas corresponde al departamento ICT de la Oficina del Secretario General.
- EURSC.eu. Credenciales para uso del personal de administración en el acceso a correo electrónico, SMS, PERSEE, Office 365 “on premise” y el resto de herramientas proporcionadas por la Oficina del Secretario General. La responsabilidad de las cuentas corresponde al departamento ICT de la Oficina del Secretario General.
- Scholae (teacher.eursc.eu, student.eursc.eu, partner.eursc.eu,...) Corresponde a las credenciales de Office 365 y SMS por parte del resto de la comunidad educativa. La responsabilidad de las cuentas corresponde al departamento ICT de la Oficina del Secretario General.

En la Escuela Europea de Alicante disponemos de distintas redes:

- Pedagógica. Aquí se encuentran los ordenadores e impresoras de aula, utilizando las credenciales de EscuelaEuropea.org
- WiFi. Red inalámbrica para la conexión del profesorado, PAS y visitas. Las credenciales, por norma general, son las mismas que en la red Pedagógica.
- Administrativa. Red administrada y gestionada por el departamento ICT de la Oficina del Secretario General, las credenciales utilizadas son las del dominio EURSC.org, EURSC.EU y SAP.

5. Normas de seguridad

A continuación, se resumen las principales obligaciones en materia de protección de datos para las personas con acceso al conjunto de tratamientos, programas, soportes y, en su caso, equipos empleados para el tratamiento de datos de carácter personal responsabilidad de **ESCUELA EUROPEA DE ALICANTE**:

- Cada usuario deberá acceder exclusivamente a aquellos datos o recursos que precise para el desarrollo de sus funciones, previa autorización del responsable del tratamiento.

Firma del usuario del sistema de información:

Nombre y Apellidos:

Fecha:

- Cada usuario será responsable de la confidencialidad de su contraseña. En caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá notificarlo como incidencia y solicitar inmediatamente el cambio de la misma.
- Las Contraseñas se almacenan de forma cifrada, es decir, de manera ininteligible. Esto significa que nadie puede saber la contraseña de un usuario, tan solo es posible cambiarla y siempre bajo petición del propio usuario, en caso de olvido o pérdida.
- Las contraseñas deberán ser suficientemente complejas y difícilmente adivinables por terceros, evitando el uso del propio identificador como contraseña o palabras sencillas, el nombre propio, fecha de nacimiento, etc.

Para ello se seguirán las siguientes pautas en la elección de las contraseñas:

- Deberán tener una longitud mínima de 8 caracteres alfanuméricos.
 - Debe contener al menos una mayúscula.
 - Debe contener al menos una minúscula.
 - Debe contener al menos un carácter especial (\$, +, #, etc.).
 - Debe tener uno o más números.
 - No deberán coincidir con el código de usuario.
 - No deberán contener nombre o apellidos del usuario.
- Tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen la confidencialidad de los datos de carácter personal.
 - Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos de carácter personal, como por ejemplo un protector de pantalla con contraseña. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.
 - En el caso de las impresoras, el usuario deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos de carácter personal. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los citados datos, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.
 - Mientras la documentación con datos de carácter personal no se encuentre archivada en los correspondientes dispositivos de almacenamiento, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se

Firma del usuario del sistema de información:

Nombre y Apellidos:

Fecha:

encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

- Los puestos de trabajo desde los que se tiene acceso a los datos de carácter personal tendrán una configuración fija en sus aplicaciones y sistema operativo que solo podrá ser cambiada bajo autorización del responsable del tratamiento.
- Queda expresamente prohibido el tratamiento de datos de carácter personal con programas ofimáticos, como procesadores de texto u hojas de cálculo, sin comunicarlo para su aprobación al responsable del tratamiento para que se proceda a implantar las medidas de seguridad adecuadas.
- Cuando los datos de carácter personal se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable del tratamiento, el usuario deberá solicitar la autorización previa del responsable del tratamiento, debiendo garantizarse, en todo caso, el nivel de seguridad adecuado al riesgo de la actividad de tratamiento.
- Cuando el usuario tenga conocimiento de cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos, deberá comunicarla sin dilación indebida al responsable del tratamiento para que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.
- Cuando el usuario tenga conocimiento de una violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, deberá comunicarla sin dilación indebida al responsable del tratamiento para que se notifique a la autoridad de control competente y, en su caso, a los interesados.
- Los soportes que contengan datos de carácter personal deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para el uso de los mismos.
- La salida de soportes informáticos y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anexos a un correo electrónico, fuera de los locales bajo el control del responsable del tratamiento deberá ser autorizada por el responsable del tratamiento. Se recomienda el uso de herramientas Cloud proporcionadas por la Escuela (OneDrive for Business o SharePoint).
- La salida de soportes informáticos y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o ajenos a un correo electrónico, deberá realizarse cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte, en aquellos

Firma del usuario del sistema de información:

Nombre y Apellidos:

Fecha:

supuestos en que la actividad de tratamiento sea considerada de alto riesgo (datos de salud, identidad sexual, etc.). Se recomienda el uso de herramientas Cloud proporcionadas por la Escuela (OneDrive for Business o SharePoint).

- Así mismo, se deberán cifrar los datos de carácter personal que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero, en aquellos supuestos en que la actividad de tratamiento sea considerada de alto riesgo. Se recomienda el uso de herramientas Cloud proporcionadas por la Escuela (OneDrive for business o SharePoint).
- El usuario deberá borrar o destruir aquellos ficheros temporales o copias de documentos que hubiese creado exclusivamente para la realización de trabajos temporales o auxiliares una vez que haya dejado de ser necesario para los fines que motivaron su creación.
- Se prohíbe el uso de dispositivos personales (portátiles, smartphones, tablets), propiedad del empleado, para el tratamiento de datos de carácter personal responsabilidad de **ESCUELA EUROPEA DE ALICANTE**, salvo que medie autorización expresa del responsable del tratamiento y previa adopción de las medidas de seguridad adecuadas al riesgo de la actividad de tratamiento.
- La **Escuela** tiene un **Protocolo para Comunicaciones** específico de obligado cumplimiento alojado en SharePoint.

6. Normas de uso del correo electrónico

Los usuarios de las cuentas de correo electrónico titularidad de **ESCUELA EUROPEA DE ALICANTE** deben cumplir las siguientes normas de uso:

- La cuenta de correo electrónico proporcionada por **ESCUELA EUROPEA DE ALICANTE** no debe ser utilizada para fines privados, personales o lúdicos, ya que constituye una herramienta de trabajo.
- Cuando se envíen mensajes de correo electrónico a múltiples destinatarios, se ha de utilizar el campo "Con Copia Oculta (CCO)" para introducir las direcciones de los mismos, a fin de salvaguardar los deberes de confidencialidad y secreto.
- Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico que previamente no hayan sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.
- Queda prohibido el envío de datos de carácter personal, en aquellos supuestos en que la actividad de tratamiento sea considerada de alto riesgo, sin aplicar mecanismos de cifrado o cualesquiera otros que garanticen que dicha información no sea accesible por persona no autorizada.

Firma del usuario del sistema de información:

Nombre y Apellidos:

Fecha:

- Queda prohibido el envío de mensajes de correo electrónico de carácter racista, xenófobo, pornográfico, sexista, de apología del terrorismo, peligroso, amenazador, difamatorio, obsceno, o que vulneren de cualquier otro modo el valor jurídico fundamental de la dignidad de la persona.
- Queda prohibido el envío de mensajes de correo electrónico que vulneren los derechos fundamentales a la protección de datos de carácter personal, a la intimidad, al honor, y/o a la propia imagen.
- Queda prohibido el envío de mensajes de correo electrónico que vulneren los derechos de propiedad intelectual o industrial.
- Queda prohibido el envío de mensajes de correo electrónico que violen cualquier otra normativa vigente.

7. Usos no aceptables

Al margen de las prohibiciones hasta aquí señaladas, tendrán la consideración de usos no aceptables (y, por ende, prohibidos) del sistema de información de **ESCUELA EUROPEA DE ALICANTE**, los siguientes:

- El uso del sistema de información de **ESCUELA EUROPEA DE ALICANTE** para fines privados, personales, lúdicos o cualesquiera otros no estrictamente relacionados con el desarrollo de sus funciones en el marco de la relación con la citada entidad, salvo que medie autorización expresa del responsable del tratamiento.
- El acceso a datos o recursos del sistema de información de **ESCUELA EUROPEA DE ALICANTE** para los que el usuario no esté debidamente autorizado por el responsable del tratamiento.
- Facilitar el acceso a datos o recursos del sistema de información de **ESCUELA EUROPEA DE ALICANTE** a personas no autorizadas.
- Compartir datos o recursos con otros usuarios autorizados sin la adopción de las medidas de seguridad adecuadas al riesgo de la actividad de tratamiento.
- La realización de acciones cuyo fin sea la obtención de contraseñas de otros usuarios autorizados, sin que medie autorización expresa del responsable del tratamiento.
- Proporcionar acceso externo desde la propia red de comunicaciones, mediante la instalación de dispositivos de acceso remoto, salvo que medie autorización expresa del responsable del tratamiento.
- La modificación no autorizada de permisos o privilegios en relación con el acceso a datos o recursos del sistema de información de **ESCUELA EUROPEA DE ALICANTE**.

Firma del usuario del sistema de información:

Nombre y Apellidos:

Fecha:

- La instalación de cualesquiera programas en los equipos del sistema de información de **ESCUELA EUROPEA DE ALICANTE** sin que medie autorización expresa del responsable del tratamiento.
- No hacer un uso racional, eficiente y considerado de los recursos proporcionados por el responsable del tratamiento, tales como: espacio en disco, memoria, redes de comunicaciones, etc.
- El uso irresponsable de las conexiones eléctricas necesarias para el buen funcionamiento de los equipos y el ecosistema técnico del aula.
- La destrucción no autorizada de datos o recursos del sistema de información de **ESCUELA EUROPEA DE ALICANTE**.
- El intento de causar cualquier tipo de daño físico o lógico al sistema de información de **ESCUELA EUROPEA DE ALICANTE**.
- Manipular o modificar el hardware (incluyendo el cableado y las conexiones físicas) de los equipos informáticos de **ESCUELA EUROPEA DE ALICANTE** sin que medie autorización expresa del responsable del tratamiento.

8. Responsabilidad

ESCUELA EUROPEA DE ALICANTE, en virtud de lo establecido en el artículo 20.3 del texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre, podrá supervisar, presencialmente o a través de cualesquiera otras herramientas o medidas de control, la estación de trabajo del usuario, en orden a comprobar la corrección de su uso de conformidad con la presente Política de Uso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.

El incumplimiento de las normas de uso del sistema de información de **ESCUELA EUROPEA DE ALICANTE**, establecidas en el presente documento, podrá tener como consecuencia la imposición de las sanciones disciplinarias correspondientes, sin perjuicio del ejercicio de las acciones laborales, civiles o penales que, en su caso, procedan y las responsabilidades que de dicho ejercicio se deriven.

Firma del usuario del sistema de información:

Nombre y Apellidos:

Fecha: