

REGISTRO DE ACTIVIDADES DEL FICHERO “CIUDADANOS EJERCIENTES DEL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA”

(Art. 30 RGPD y Art. 31 LOPDGDD)

FICHERO	CIUDADANOS EJERCIENTES DEL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA DEL COLEGIO DE VETERINARIOS
NOMBRE Y DATOS DE CONTACTO DEL RESPONSABLE	COLEGIO OFICIAL DE VETERINARIOS DE ÁVILA C.I.F.Q1371001G Calle San Juan de la Cruz, 26, C.P. 05001, Ávila - España Teléfono: 920 22 17 82 e-mail: colvetavila@gmail.com
CORRESPONSABLES	NO APLICA
REPRESENTANTE DEL RESPONSABLE	NO APLICA
DELEGADO DE PROTECCIÓN DE DATOS	dpd.colvetavila@gmail.com
ACTIVIDAD DEL TRATAMIENTO	TRATAMIENTO DE LOS DATOS IDENTIFICATIVOS DE LOS CIUDADANOS QUE EJERCEN SU DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA DEL COLEGIO.
FINALIDAD	<ul style="list-style-type: none">○ Finalidad principal: gestionar las solicitudes de acceso a la información pública del Colegio.○ Finalidad secundaria: envío de la resolución en la que se conceda o deniegue el acceso a la información pública del Colegio.○ Los datos personales de los ciudadanos solicitantes no serán tratados posteriormente de manera incompatible con los fines descritos en el párrafo anterior. En ningún caso se elaborarán perfiles ni decisiones automatizadas con estos datos personales.
BASE JURÍDICA	La base legal para el tratamiento de los datos es el cumplimiento de una obligación legal del Art.6.1.c. RGPD , concretamente, la “Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno”; así como en la normativa legal autonómica “Ley 3/2015, de 4 de marzo, de

REGISTRO DE ACTIVIDADES DEL FICHERO “CIUDANOS EJERCIENTES DEL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA”

(Art. 30 RGPD y Art. 31 LOPDGDD)

	Transparencia y Participación Ciudadana de Castilla y León” y “Decreto 7/2016, de 17 de marzo, por el que se regula el procedimiento para el ejercicio del derecho de acceso a la información pública en la Comunidad de Castilla y León”.	
CATEGORÍAS DE INTERESADOS	CIUDADANOS QUE EJERCEN SU DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA DEL COLEGIO	
CATEGORÍAS DE DATOS PERSONALES	<ul style="list-style-type: none"> ○ DATOS IDENTIFICATIVOS (Nombre completo y DNI) ○ DATOS DE CONTACTO (correo electrónico o dirección postal) 	
CESIONES DE DATOS	NO APLICA	
COMUNICACIÓN DE DATOS	Los datos del ciudadano solicitante no serán comunicados a otras entidades u organizaciones, si bien, podrá tener acceso a los mismos, proveedores de servicios legales del Colegio, con la finalidad de atender y gestionar legalmente la solicitud de acceso a la información pública u organismos de la Administración Pública habilitados a tal efecto. Si desea información detallada sobre los datos identificativos de esta entidad puede solicitarla en colvetavila@gmail.com	
TRANSFERENCIA INTERNACIONAL DE DATOS	TERCER PAÍS	BASE PARA LA TRANSFERENCIA
	NO APLICA	PAÍS DESTINATARIO DECLARADO DE NIVEL DE PROTECCIÓN ADECUADO NO APLICA
		ALTERNATIVAS A LA FALTA DE DECISIÓN DE ADECUACIÓN, GARANTÍAS ADECUADAS NO APLICAN
		AUTORIZACIÓN EXPRESA DE LA AEPD NO APLICA
PLAZO PREVISTO PARA LA SUPRESIÓN	Los datos personales proporcionados se conservarán 5 años desde la baja de forma voluntaria o por defunción del colegiado.	

REGISTRO DE ACTIVIDADES DEL FICHERO “CIUDANOS EJERCIENTES DEL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA”

(Art. 30 RGPD y Art. 31 LOPDGDD)

	MEDIDAS TÉCNICAS	MEDIDAS ORGANIZATIVAS
MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD	<ol style="list-style-type: none"> 1. Política de contraseñas robusta a nivel del sistema, tanto para el acceso al sistema operativo como a las aplicaciones. 2. Antivirus implantado y configurado. 3. Configurados los sistemas para la actualización automática del sistema operativo y las aplicaciones. 4. Limitada la utilización de usuarios genéricos. 5. Limitados los permisos de administración. 6. Configurado el bloqueo de sesión por inactividad en sistemas y aplicaciones. 7. Restringidos los puertos USB a puestos determinados 8. Dispositivos destructores de documentación. 9. Limitada la navegación a páginas de ciertos contenidos. 10. Controlado y prohibido el acceso remoto hacia la propia organización. 11. Habilitados mecanismos de seguridad en la impresión de documentos. 12. Limitado el acceso a la red corporativa a los equipos que no estén debidamente protegidos. 	<ol style="list-style-type: none"> 1. Obligación de mantener confidencialidad. 2. Obligación de notificar cualquier incidente. 3. Prohibición de publicar o compartir contraseñas 4. Obligación de bloquear la sesión al ausentarse del puesto de trabajo y apagar el equipo al finalizar la jornada laboral. 5. Limitación en el uso de servicios de almacenamiento online. 6. Uso adecuado de los medios de almacenamiento extraíble 7. Prohibición de la alteración de la configuración del equipo y la instalación de aplicaciones no autorizadas. 8. Obligación de guardar la documentación de trabajo al ausentarse del puesto de trabajo y al terminar la jornada laboral (Política de mesas limpias) 9. Obligación de destruir la documentación mediante mecanismos seguros. 10. Obligación de no abandonar documentación en las impresoras o escáneres. 11. Instrucciones de utilización de internet y correo electrónico corporativo. 12. Instrucciones de utilización de dispositivos personales.