POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ENS – RD 311/2022

Consell Valencià
de Col.legis Veterinaris

DOCUMENTO			
	Tipo	**Grupo**	**Nombre**
Identificación del documento	Política	Articulado y medidas de seguridad	Política de Seguridad de la Información

REGISTRO DE CAMBIOS		
Elaborado	**Revisado por**	**Aprobado por**
Comité de Seguridad	Comité de Seguridad	Dirección

VERSIÓN	FECHA	MOTIVO CAMBIO
1	13/01/2025	Versión inicial

Tabla de contenido

1. INTRODUCCIÓN

El **Consell Valencià de Col·legis Veterinaris** (en adelante, CVCV), como órgano que coordina a los Colegios Oficiales de Veterinarios de la Comunitat Valenciana y tiene, a todos los efectos, la condición de corporación de derecho público, con personalidad jurídica propia y plena capacidad para el cumplimiento de sus fines, el cual depende de los sistemas TIC (Tecnologías de la Información y Comunicaciones) para el ejercicio de sus funciones, estando directamente relacionado a través de los medios electrónicos, entre otros, con Administraciones Públicas y Organismos Oficiales.

Estos sistemas TIC deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información tratada o de los servicios prestados y todo ello, con la finalidad de garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes de seguridad que se produzcan.

En definitiva, los sistemas TIC de CVCV deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, uso previsto y valor de la información y los servicios, estando preparados para prevenir, detectar, reaccionar y recuperarse de incidentes.

Para defenderse de estas amenazas, se requiere una estrategia que permita adaptarse a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que, sin perjuicio de las medidas ya adoptadas, tanto CVCV como su personal deban aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (RD 311/2022 de 3 de mayo, en adelante también ENS), así como realizar un seguimiento continuo de los niveles de prestación de los servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes que se produzcan para garantizar la continuidad de los servicios prestados.

Es por ello que CVCV debe tomar conciencia de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida de cada uno de los Sistemas de Información existentes en CVCV, desde su concepción hasta su retirada de servicio, pasando por las fases de desarrollo o adquisición y las actividades de explotación. Asimismo, se tendrá en cuenta que los requisitos de seguridad y las necesidades de financiación de los mismos, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en los pliegos de licitación para proyectos de TIC.

Para ello, en cumplimiento de lo previsto en el artículo 12 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y con el objeto de asegurar que esta comunicación e intercambio de información se realice con la adecuada seguridad, garantizando la custodia de la misma de acuerdo con sus especificaciones funcionales, su disponibilidad e integridad, así como evitando que ésta llegue al conocimiento de personas no autorizadas, se elabora la presente Política de Seguridad de la Información, sobre la base de los siguientes principios básicos:

a) **Seguridad integral**: La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el Sistema.

b) **Gestión de riesgos**: El análisis y gestión de riesgos será una parte esencial del proceso de seguridad.

c) **Prevención, reacción y recuperación**: Eliminando o, al menos, reduciendo la probabilidad de que las amenazas lleguen a materializarse con perjuicio para el Sistema, acompañando a las medidas de detección de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo y estableciendo medidas de recuperación que permitan la restauración de la información y servicios.

d) **Líneas de defensa**: El Sistema dispondrá de una estrategia de protección constituida por varias capas de seguridad de modo que en caso de que una falle se gane tiempo para la reacción adecuada frente a incidentes que no hayan podido evitarse, se reduzca la probabilidad de que el Sistema sea comprometido en su conjunto y se minimice el impacto final sobre el mismo.

e) **Revaluación periódica**: Las medidas de seguridad se revaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

f) **Función diferenciada**: En los sistemas de información se diferenciará el responsable de la información/servicio y el responsable de la seguridad (principio de segregación de funciones).

2. OBJETIVO Y ALCANCE

Esta POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN recoge las normas relativas a las medidas de seguridad que CVCV debe emplear tanto en el tratamiento de datos personales como en el uso de sistemas TIC, siendo esa la finalidad de este documento y de la normativa de desarrollo que dicten los órganos directivos de la organización.

Esta Política se aplica a todo el Sistema de Gestión de Seguridad de la Información (SGSI).

Los usuarios de este documento son las personas trabajadoras de CVCV, así como también terceros externos a la organización, dentro del alcance del SGSI y del ámbito del ENS.

CVCV depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad o trazabilidad de la información tratada o los servicios prestados. El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

3. TERMINOLOGÍA BÁSICA SOBRE SEGURIDAD DE LA INFORMACIÓN

- **Confidencialidad**: característica de la información por la cual solo está disponible para personas o sistemas autorizados.
- **Integridad**: característica de la información por la cual solo que es modificada por personas o sistemas autorizados y de una forma permitida.
- **Disponibilidad**: característica de la información por la cual solo pueden acceder las personas autorizadas cuando sea necesario.
- **Autenticidad**: característica de la información por la cual el hecho de que quien accede al servicio es realmente quien es.
- **Trazabilidad**: característica de la información por la cual se puede rastrear a posteriori quien ha accedido o modificado una cierta información asociada al servicio, quedando constancia del acceso.
- **Seguridad de la información**: es la preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Sistema de gestión de seguridad de la información**: parte de los procesos generales de gestión que se encarga de planificar, implementar, mantener, revisar y mejorar la seguridad de la información.

4. PREVENCIÓN, DETECCIÓN, REACCIÓN Y RESPUESTA

El CVCV debe estar preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 8 del ENS.

2.1. PREVENCIÓN

Los departamentos 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. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, se debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben 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 a distintos niveles. Por tanto, se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. RESPUESTA

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

- Ponerse en contacto con las Fuerzas y Cuerpos de Seguridad según los procedimientos específicos previstos.
- Establecer comunicación con los cuerpos de emergencias y protección civil.

2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, CVCV debe desarrollar planes de continuidad de los sistemas como parte de su plan general de continuidad de negocio y actividades de recuperación.

5. ALCANCE

3.1. AMBITO SUBJETIVO

La presente Política de Seguridad de la Información es de aplicación a todos los miembros de la plantilla de CVCV, y en particular a aquellos que utilicen, operen y administren los sistemas de información y comunicaciones.

De acuerdo con lo anterior, todo el personal de CVCV tiene la obligación de conocer y cumplir la misma.

Asimismo, será de aplicación, en los términos y condiciones previstos en el apartado 13, a aquellos terceros en los que concurra alguno de estos supuestos:

(i) Terceros organismos para los que CVCV preste servicios o de los que maneje información.

(ii) Terceros prestadores de servicios a CVCV o a los que se les ceda información.

3.2. AMBITO OBJETIVO

Esta Política se aplica a todos los sistemas TIC de CVCV, relacionados con las funciones que le son atribuidas por la legislación vigente.

Específicamente se aplica a los sistemas que dan soporte a su cadena de valor, al ejercicio de derechos y cumplimiento de deberes por medios electrónicos, y a la interacción por medios electrónicos con los ciudadanos y la Administración Pública.

6. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

6.1. OBJETIVOS Y MEDICIÓN

Los objetivos generales para el sistema de gestión de seguridad de la información son gestionar y cumplir los requerimientos en materia de seguridad de la información propios de CVCV y de las diferentes partes interesadas (clientes, proveedores, personal y otros), así como crear una mejor imagen y sus servicios prestados.

El Responsable de Seguridad es el responsable de revisar y de establecer nuevos objetivos de seguridad para cada ciclo del Sistema de Gestión de Seguridad de la Información – SGSI –, Sistema de Gestión de la Seguridad del Esquema Nacional de Seguridad – ENS – (en adelante, referidos indistintamente como "SGSI".

CVCV medirá el cumplimiento de los objetivos establecidos para el SGSI. El Responsable de Seguridad es el responsable de definir el método para medir el cumplimiento de los objetivos; la medición se realizará al menos al menos una vez al año y el Responsable de Seguridad analizará y evaluará los resultados y los reportará a Dirección General como material para la revisión por parte de la Dirección.

6.2. MISIÓN

Son fines propios del Consell Valencià de Col·legis de Veterinaris:

a) La coordinación de los colegios profesionales de la Comunitat Valenciana y la representación y la defensa de la profesión veterinaria en cuestiones de ámbito autonómico.

b) Relacionarse, en nombre de la profesión, con las instituciones de la Generalitat Valenciana, en particular con el Gobierno Valenciano, al objeto de facilitar la mutua colaboración y entendimiento para la mejor satisfacción de los intereses sociales y profesionales.

c) La colaboración con los poderes públicos en la consecución de la salud de las personas y animales, mejora de la ganadería y la más eficiente, justa y equitativa regulación y ordenación del sector ganadero y alimentario desde la fase de producción al consumo; así como la atención al medio ambiente, la protección de los consumidores, y la conservación, protección y bienestar animal.

d) La elaboración y promoción de las normas deontológicas de la profesión.

El Consell Valencià de Col·legis de Veterinaris tiene las siguientes funciones:

a) Elaborar, aprobar y modificar sus propios estatutos y reglamentos de régimen interior.

b) Elaborar las normas deontológicas comunes a la profesión Veterinaria y velar por su cumplimiento, sin perjuicio de las competencias de cada colegio miembro.

c) Resolver en vía administrativa los recursos que se interpongan contra los actos y acuerdos de los colegios.

d) Aprobar sus presupuestos, regular y fijar proporcionalmente al número de colegiados la participación de los colegios en los gastos del Consejo.

e) Informar con carácter preceptivo y no vinculante sobre todos los proyectos de normas del Gobierno Valenciano que afecten a los colegios de veterinarios o a la propia profesión.

f) Mantener los contactos oportunos con otras organizaciones de ámbito estatal o internacional relacionadas con la profesión veterinaria, con otros consejos de la Organización Colegial Veterinaria, así como con otros consejos de colegios profesionales.

g) Ejercer las funciones disciplinarias con respecto a los miembros del propio Consejo Valenciano y los de las juntas de gobierno de los colegios de esta Comunidad.

h) Participar en los consejos y órganos consultivos de la administración valenciana, a cuyos efectos corresponderá al Consejo Valenciano de Colegios de Veterinarios la designación de sus representantes.

i) Determinar los modelos de sellos, pólizas, documentos y demás impresos utilizados en la actividad profesional de los veterinarios.

j) Formular propuestas normativas, reformas o medidas para el desarrollo y perfeccionamiento de las actuaciones propias de la profesión veterinaria.

k) Participar con los poderes públicos en cuantas actuaciones afecten a la veterinaria de salud pública, al medio ambiente, a la higiene alimentaria, a la producción animal, al desarrollo ganadero y a la conservación, protección y bienestar animal.

l) Informar preceptivamente, con carácter previo a su aprobación por la Generalitat Valenciana, los proyectos de fusión, absorción, segregación, disolución y cambio de denominación de los Colegios de Veterinarios de la Comunidad Valenciana.

m) Aquellas funciones de los colegios provinciales que éstos deleguen en el Consejo Valenciano de Colegios de Veterinarios.

n) Fomentar, crear y organizar instituciones, servicios y actividades que, siempre en relación con la profesión, tengan por objeto la promoción cultural y científica, la prestación social y sanitaria, la cooperación y el mutualismo, el fomento de la ocupación y otras actuaciones pertinentes, así como establecer los conciertos o acuerdos más apropiados en este sentido con la administración y las instituciones y entidades públicas y privadas que corresponda.

o) Suscribir convenios con la Generalitat Valenciana, así como con otras instituciones públicas o privadas.

p) Dirimir los conflictos que puedan suscitarse entre los colegios, sin perjuicio del ulterior recurso contencioso administrativo.

q) Construir o participar en consorcios públicos o en fundaciones, asociaciones y otras entidades, así como establecer relaciones de cooperación con entidades públicas o privadas.

r) Las demás que le atribuyan otras leyes y todas aquellas que, no expresamente enunciadas, sean concomitantes o consecuencia de las anteriores.

7. MARCO NORMATIVO

CVCV, como órgano que coordina a los Colegios Oficiales de Veterinarios de la Comunitat Valenciana y tiene, a todos los efectos, la condición de corporación de derecho público, con personalidad jurídica propia y plena capacidad para el cumplimiento de sus fines, se rige por la siguiente legislación:

a) RESOLUCIÓN de 9 de noviembre de 1999, de la secretaria general de la Conselleria de Justicia y Administraciones Públicas, por la que se inscriben los Estatutos del Consejo Valenciano de Colegios de Veterinarios.

b) Ley 6/1997, de 4 de diciembre, de Consejos y Colegios Profesionales de la Comunidad Valenciana y demás normas que la desarrollen.

c) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

d) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

e) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

f) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

g) 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, RGPD).

h) Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI-CE).

i) Ley 59/2003, de 19 de diciembre, de firma electrónica.

En todo caso, lo anterior se entenderá sin carácter limitativo y sin perjuicio de lo regulado en cualquier otra normativa que resulte de aplicación.

Esta Política, y todo el SGSI, deben cumplir los requisitos legales y normativos importantes para la organización en el ámbito de la seguridad de la información, como también con las obligaciones contractuales.

También se tendrá en consideración la normativa que le sea de aplicación en cada momento, en base a lo dispuesto en el Código de Ciberseguridad. Asimismo, cada vez que se actualice este código, a través del servicio **Mi BOE** se recibirán alertas e información por sobre las novedades publicadas y se revisará y tendrán en cuentan las que sean de interés para la organización.

8. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Dirección General de CVCV, en el ejercicio de las funciones de dirección y gestión ordinaria de la entidad, es la máxima responsable del impulso y cumplimiento de lo previsto en la presente Política de Seguridad de la Información y demás normas, guías y procedimientos de seguridad que, en el desarrollo de la misma, se aprueben.

Para la organización, gestión, y coordinación de la seguridad de la información dentro de CVCV se dispone de la siguiente estructura con las funciones y responsabilidades que, asimismo, a continuación, se detallan:

1. Responsable de Seguridad.
2. Responsable de Sistemas.
3. Responsable de la Información.
4. Responsable del Servicio.
5. Administrador de Seguridad del Sistema.

En caso de conflicto entre los distintos órganos que tienen encomendadas competencias en materia de seguridad de la información éstos serán resueltos por el superior funcional.

3.1. ROLES: FUNCIONES Y RESPONSABILIDADES

3.1.1. RESPONSABLE DE SEGURIDAD

El Responsable de Seguridad, será el representante de CVCV en materia de Seguridad de la Información y será responsable de:

a) Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información de CVCV, de acuerdo con lo establecido en la Política de Seguridad de la Información de CVCV.

b) Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Sus funciones son las siguientes:

- Atender los requerimientos de CVCV en materia de seguridad de la información.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de CVCV en lo que respecta a seguridad de la información.

- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que son consistentes y alineados con la estrategia decidida en la materia.
- Elaborar la Política de Seguridad de la información y proponer su aprobación al órgano superior competente, así como revisarla como mínimo anualmente planteando las posibles modificaciones que estime convenientes a dicho órgano.
- Aprobar la normativa de seguridad de la información.
- Promover, elaborar y aprobar los requisitos de formación a todo el personal de CVCV desde el punto de vista de seguridad de la información.
- Recabar la información sobre los principales riesgos residuales asumidos por CVCV y recomendar posibles actuaciones respecto de ellos.
- Dar soporte, supervisar y requerir información sobre el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de CVCV en materia de seguridad de la información.
- Aprobar planes de mejora de la seguridad de la información de CVCV.
- Priorizar las actuaciones en materia de seguridad de la información.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables de CVCV, elevando a la Dirección General aquellos casos que se estimen oportunos.
- Supervisar el mantenimiento de la seguridad de la información manejada y de los servicios prestados por los sistemas de información de CVCV.

- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos.
- Determinar la categoría del sistema o sistemas según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Elaborar la Normativa de Seguridad de la Información de CVCV.
- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Colaborar conjuntamente con el Responsable del Sistema en el diseño de planes de mejora de la seguridad de la información.
- Coordinar con los distintos responsables que las medidas de seguridad de la información establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Aprobar los procedimientos de seguridad de la información elaborados por el Responsable del Sistema.

En particular, y con el objeto de garantizar la debida coordinación entre las distintas personas con responsabilidades en materia de seguridad de la información, el Responsable de Seguridad:

- Informa a los Responsables de la Información de los incidentes ocurridos en materia de seguridad y las medidas adoptadas para la mitigación de sus impactos, que afecten a la Información de su competencia y, en particular, de la estimación de los riesgos residuales y de sus variaciones significativas respecto de los anteriormente conocidos y aprobados.
- Informa a los Responsables de Servicio de los incidentes ocurridos en materia de seguridad y las medidas adoptadas para la mitigación de sus impactos, que afecten al Servicio de su competencia y, en particular, de la estimación de los riesgos residuales y de sus variaciones significativas respecto de los anteriormente conocidos y aprobados.

Cuando, en atención a la complejidad, distribución, separación física o número de usuarios de los sistemas de información, sea necesario personal adicional para llevar a cabo las funciones del Responsable de Seguridad, éste podrá designar cuantos responsables de Seguridad Delegados considere necesarios. Dicha designación deberá ser efectuada con carácter formal y comportará la delegación de funciones, pero no de su responsabilidad.

3.1.2. RESPONSABLE DE LA INFORMACIÓN

El Responsable de la Información es la persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad, es decir, de determinar los niveles de seguridad de la información, teniendo la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.

Sus funciones son:

- Clasificar la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad).

  La aprobación de los niveles de seguridad se realizará a propuesta del Responsable de Seguridad oído el Responsable del Sistema.

- Validar los preceptivos análisis de riesgos y, junto a los Responsables de los Servicios y contando con la participación y asesoramiento del Responsable de Seguridad y del Responsable del Sistema, seleccionar las salvaguardas a implantar.
- Aceptar, junto con los Responsables de los Servicios, los riesgos residuales calculados en el análisis de riesgos, y realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

3.1.3. RESPONSABLE DEL SERVICIO

El Responsable del Servicio es la persona que tiene la potestad de establecer los requisitos del servicio en materia de seguridad, es decir, de determinar los niveles de seguridad de los servicios, teniendo la responsabilidad última del uso que se haga de un determinado servicio y, por tanto, de su protección.

Sus principales funciones son:

- Determinar los niveles de seguridad del servicio en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad).

  La aprobación de los niveles de seguridad se realizará a propuesta del Responsable de Seguridad oído el Responsable del Sistema.

- Validar los preceptivos análisis de riesgos y, junto a los Responsables de la Información y contando con la participación y asesoramiento del Responsable de Seguridad y del Responsable del Sistema, seleccionar las salvaguardas a implantar.
- Aceptar, junto con los Responsables de la Información, los riesgos residuales calculados en el análisis de riesgos, y realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

3.1.4. COMITÉ DE SEGURIDAD

Es el órgano colegiado dependiente que se encarga de ejecutar, desarrollar, implantar, supervisar, auditar y proponer a aquél la Política de Seguridad de la Información dentro de CVCV.

Entre sus funciones podemos destacar:

- Atender las inquietudes de la Dirección General y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección General.
- Garantizar que el SGSI sea implementado y mantenido de acuerdo con esta Política y garantizar que todos los recursos necesarios estén disponibles.
- Promover la mejora continua del Sistema de Gestión.
- Elaborar la estrategia de evolución de la Organización en lo que respecta a la seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para que sea aprobada por la Dirección.
- Elaborar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Unidad Organizativa y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.

- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Desarrollar planes de mejora de la seguridad de la información de la entidad. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Velar por que la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

3.1.5. RESPONSABLE DEL SISTEMA

Conforme al ENS, es necesario nombrar formalmente a una única persona en la organización (no puede ser un órgano colegiado, aunque puede delegar) que se encarga de desarrollar, operar y mantener los sistemas TIC durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento de CVCV.

Es la persona responsable de:

- Desarrollar, operar y mantener el Sistema (entendiendo como tal el conjunto de sistemas de información de CVCV) durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la política de gestión del Sistema estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Acordar la suspensión del manejo de una cierta Información o la prestación de un cierto Servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

Sus principales funciones son:

- Elaborar los procedimientos operativos de seguridad de la información.
- Colaborar conjuntamente con el Responsable de Seguridad en el diseño de planes de mejora de la seguridad.
- Elaborar el Plan de Continuidad del Sistema.
- Velar por el cumplimiento de las obligaciones del Administrador de Seguridad del Sistema.

- Investigar los incidentes de seguridad que afecten al sistema y comunicarlos al Responsable de Seguridad.

En particular, y con el objeto de garantizar la debida coordinación entre las distintas personas con responsabilidades en materia de seguridad de la información, el Responsable del Sistema:

- Reporta al Responsable de Seguridad:
    - De las actuaciones en materia de seguridad, en particular, lo relativo a decisiones de arquitectura de sistema.
    - Resumen consolidado de incidentes de seguridad.
    - De la eficacia de las medidas de protección que se deben implantar

Cuando en atención a la complejidad, distribución, separación física o número de usuarios de los sistemas de información, sea necesario personal adicional para llevar a cabo las funciones del Responsable del Sistema, éste podrá designar cuantos responsables del Sistema Delegados considere necesarios. Dicha designación deberá ser previamente aprobada por el Comité de Seguridad de la Información, efectuada con carácter formal y comportará la delegación de funciones, pero no de su responsabilidad.

3.1.6. ADMINISTRADOR DE LA SEGURIDAD DEL SISTEMA

Es el responsable de implantar, gestionar y mantener las medidas de seguridad aplicables al Sistema de Información.

Sus principales funciones y responsabilidades son:

- Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad de los Sistemas de Información.
- Implantar, gestionar y mantener las medidas de seguridad aplicadas en los Sistemas de Información.
- Supervisar que las medidas de seguridad son aplicadas estrictamente.
- Monitorizar el estado de la seguridad del Sistema.
- Gestionar las autorizaciones concedidas a los usuarios del Sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el Sistema se ajusta a lo autorizado.
- Aplicar los Procedimientos Operativos de Seguridad de la Información y Explotación de los Sistemas de Información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Informar al Responsable de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

3.2. OTROS PERFILES EXISTENTES

3.2.1. Delegado de Protección de Datos (DPD)

El DPD será designado conforme al artículo 37 del RGPD y desempeñará las funciones indicadas en el artículo 39 del RGPD y la normativa de protección de datos en vigor.

3.2.2. Usuarios

Se considerará usuario al personal de CVCV, el cual tendrá la obligación de conocer y cumplir la presente Política.

3.2.3. Terceros

A toda organización que preste servicios o gestione información de CVCV, se le hará partícipe de la presente Política.

3.3. PROCEDIMIENTOS DE DESIGNACIÓN

La Dirección General de CVCV es el órgano competente para:

- El nombramiento del Responsable de Seguridad y su sustituto.
- El nombramiento de los Responsables de la Información.
- El nombramiento de los Responsables del Servicio.
- El nombramiento del Responsable del Sistema.
- El nombramiento de los Administradores de Seguridad del Sistema.

9. DATOS DE CARÁCTER PERSONAL

En el desarrollo de las funciones encomendadas, CVCV trata datos de carácter personal, contando, en cumplimiento de la normativa de aplicación, con un Registro de Actividades del Tratamiento, en el que se recogen los tratamientos llevados a cabo por la entidad.

Todos los sistemas de información de CVCV se ajustarán a los niveles de seguridad requeridos, así como de las indicaciones del Delegado de Protección de Datos.

10. GESTIÓN DE RIEGOS

Respecto de todos los sistemas de información comprendidos en el alcance de esta Política se deberá realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el artículo 6 del mismo.

Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Responsable de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

El Responsable de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

11. AUDITORÍA

De acuerdo con lo establecido en el artículo 31 del ENS, los sistemas de información de CVCV se someterán a una auditoría en base a los siguientes periodos y criterios:

- **Ordinaria**: periodo bienal.
- **Extraordinaria**: siempre que se produzcan modificaciones sustanciales en el Sistema de Información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

12. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información se desarrollará mediante documentos más precisos que ayuden a llevar a cabo lo propuesto. Para ello se utilizarán:

- Normas de seguridad.
- Guías de seguridad.
- Procedimientos de seguridad.

Las normas de seguridad uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.

Las guías tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad. Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.

13. CONCIENCIACIÓN Y FORMACIÓN

Con el objetivo de lograr la plena conciencia respecto a que la Seguridad de la Información afecta a todos los miembros de la plantilla de CVCV y a todas las actividades, de acuerdo al principio de Seguridad Integral recogido en el artículo 5 del ENS, el Responsable de Seguridad establecerá un programa de concienciación continua a todos los miembros de la plantilla de CVCV, en particular a los de nueva incorporación.

Asimismo, el Responsable de Seguridad elaborará y aprobará los requisitos de formación necesarios desde el punto de vista de seguridad de la información.

14. OBLIGACIONES DEL PERSONAL

Todos los miembros de CVCV tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Responsable de Seguridad disponer los medios necesarios para que la información llegue a los afectados, utilizando según las posibilidades de CVCV los mismos canales para la concienciación y formación del sistema de gestión de la calidad implantado en la fundación.

15. TERCERAS PARTES

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

Cuando CVCV utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad de la Información 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 esta Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se solicitará un informe del Responsable de Seguridad que concrete los riesgos en que se incurre y la forma de tratarlos. Será necesaria la aprobación de este informe por parte de los responsables de la información y los servicios afectados, previamente al uso de los servicios de terceros o cesión de información a los mismos.

16. ORGANIZACIÓN E IMPLANTACIÓN DEL PROCESO DE SEGURIDAD

La seguridad deberá comprometer a todas las personas pertenecientes a CVCV. Asimismo, se procede a una organización y distribución de funciones, responsabilidades y roles.

17. GESTIÓN DEL PERSONAL Y PROFESIONALIDAD

Todo el personal relacionado con la información y los sistemas será informado y formado en los deberes, obligaciones y responsabilidades en materia de seguridad.

Todos los roles definidos en la presente política ejercerán sus puestos con la debida profesionalidad.

18. AUTORIZACIÓN Y CONTROL DE ACCESOS

Se establecen los mecanismos necesarios de protección que controlen el acceso a los sistemas de información, a través de la mejora continua. Estos accesos estarán limitados a las personas usuarias, procesos, dispositivos u otros sistemas de información, debidamente autorizados para el desempeño de las funciones atribuidas.

19. PROTECCIÓN DE LAS INSTALACIONES

Se procurará que los sistemas de información y su infraestructura de comunicaciones asociada se ubiquen en áreas controladas que sean emplazamientos seguros, y que sean protegidos bien por controles de acceso físicos adecuados a su nivel de criticidad o mediante medidas apropiadas a los mismos, que garanticen su protección en función los requisitos legales y normativos existentes.

20. ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD

En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser utilizados, se tendrán en cuenta aquellos que ofrezcan garantías de seguridad adecuadas para el cumplimiento de sus funciones.

21. MÍNIMO PRIVILEGIO

Se diseñarán y configurarán los sistemas de la información otorgando los mínimos privilegios para su correcto desempeño.

22. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

Todo elemento físico o lógico requiere autorización previa a su instalación en el sistema.

23. PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO

Se prestará especial atención a la información almacenada o en tránsito a través de equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas.

24. COMUNICACIÓN DE LA POLÍTICA

El Responsable de Seguridad debe asegurarse de que todas las personas trabajadoras de CVCV, así como también los participantes externos correspondientes, dentro del alcance estén familiarizados con esta Política.

25. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

26. REQUISITOS MÍNIMOS DE REGISTRO DE ACTIVIDAD

Con la finalidad exclusiva de lograr el cumplimiento del objeto de esta política de seguridad de la información y protección de datos personales, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de las personas afectadas, y de acuerdo con la normativa sobre protección de datos personales y demás disposiciones que resulten de aplicación, se podrán registrar las actividades de las personas usuarias, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo a la persona que actúa.

27. PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS

Se podrá proteger al sistema de las conexiones a redes públicas, no estando permitida la conexión a las mismas por parte para los usuarios, entendiendo por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público, de conformidad a la definición establecida en el apartado 32 del anexo II, de la Ley 9/2014, de 9 de mayo, de Telecomunicaciones.

En todo caso, se podrán analizar los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se podrá controlar su punto de unión.

28. OBLIGACIONES

Todos los miembros de CVCV tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

29. IMPLEMENTACIÓN Y MEJORA CONTINUA DEL SGSI

A través de la presente Política, la Dirección General declara que en la implementación y mejora continua del SGSI se contará con el apoyo de los recursos adecuados para lograr todos los objetivos establecidos en esta Política, como también para cumplir con todos los requisitos identificados.

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por y difundida para que la conozcan todas las partes afectadas.

30. PUBLICIDAD

Con el objeto de garantizar la máxima difusión de la Política de Seguridad de la Información entre los empleados y empleadas de CVCV se procederá a la publicación de la misma en la carpeta “7 RIVIA ENS” del servidor y/o intranet RIVIA-CVCV y RIVIA-Colegios.

Asimismo, serán objeto de publicación en el repositorio de la entidad las normas, guías y procedimientos de seguridad que en desarrollo del ENS se aprueben. Lo anterior podrá verse excepcionado respecto de aquellos documentos que por su contenido sean calificados de confidenciales.

31. APROBACIÓN Y ENTRADA EN VIGOR

La presente Política de Seguridad de la información será revisada como mínimo una vez al año de modo que se garantice su adaptación a las nuevas circunstancias, técnicas u organizativas, que pudieran surgir.

Esta Política de Seguridad de la información es efectiva desde su fecha de aprobación y hasta que sea reemplazada por una nueva Política.

Texto aprobado por la Dirección de Consell Valencià de Col·legis Veterinaris en sesión de 13 de enero de 2025.

Firmado por Dirección
 Fdo. Inmaculada Ibor Martínez