POLÍTICA DE SEGURIDAD

ILUSTRE COLEGIO OFICIAL VETERINARIO DE CANTABRIA

ADO DE REVISIÓN/MODIFICACIÓN DEL DOCUMENTO		
Nº edición	**Fecha**	**Naturaleza de la Revisión**
0	25/10/2024	Edición inicial

Texto aprobado en la fecha indicada en el cuadro. El documento es efectivo desde dicha fecha y hasta que sea reemplazado por una nueva versión. Este texto anula el anterior, que fue aprobado según indicaciones del cuadro anterior

ÍNDICE

1. ENTRADA EN VIGOR

Esta Política se Seguridad de la Información es efectiva desde la fecha de aprobación arriba indicada y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

El Ilustre Colegio Oficial Veterinario de Cantabria (en adelante, **LA EMPRESA**) 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 o confidencialidad 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.

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, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, 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.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

Los departamentos deben estar preparados 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, los departamentos deben:

- 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 según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce 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).

3. ALCANCE

Esta política se aplica a todos los sistemas TIC de **LA EMPRESA** y a todos los miembros de la organización, sin excepciones.

4. PRINCIPIOS BÁSICOS

La presente política de seguridad se establece de acuerdo con los principios básicos señalados en el capítulo II del RD 311.2022 y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

b) Análisis y gestión de los riesgos.

c) Gestión de personal.

d) Profesionalidad.

e) Autorización y control de los accesos.

f) Protección de las instalaciones.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad.

h) Mínimo privilegio.

i) Integridad y actualización del sistema.

j) Protección de la información almacenada y en tránsito.

k) Prevención ante otros sistemas de información interconectados.

l) Registro de la actividad y detección de código dañino.

m) Incidentes de seguridad.

n) Mejora continua del proceso de seguridad.

Estos requisitos mínimos se exigen en proporción a los riesgos identificados en nuestro sistema, de conformidad con lo dispuesto en el artículo 28 del RD 311.2022.

5. MISIÓN

LA EMPRESA se compromete a prestar sus servicios de forma gestionada y cumpliendo con los requisitos establecidos en su Sistema de Gestión de modo que se garantice un servicio ininterrumpido conforme a los requisitos de disponibilidad, seguridad y calidad hacia los usuarios.

Debido a nuestra actividad, en **LA EMPRESA** sabemos que la información es un activo con un elevado valor para nuestra organización y sobre todo la de nuestros usuarios y requiere, por lo tanto, una protección y gestión adecuadas con el fin de dar continuidad al servicio principal de Registro de Animales de Compañía en Cantabria y minimizar los posibles daños ocasionados por fallos en la Seguridad de la Información.

Para ello, la organización busca cumplir los siguientes objetivos:

- Proteger adecuadamente la confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad de sus activos de información mediante la introducción de una serie de controles para gestionar los riesgos de seguridad relevantes.
- Priorizar la protección y salvaguarda de sus usuarios y los datos de los usuarios como una prioridad de negocio.

- Establecer, implementar, monitorear, mantener y mejorar continuamente su gestión de seguridad de la información como parte de su enfoque más amplio de gestión empresarial, y mantener la Certificación Acreditada a los estándares adecuados.
- Gestionar cualquier violación de la seguridad de la información de manera oportuna y responsable, e invertirá en estrategias adecuadas de detección, respuesta y remediación.
- A intervalos planificados, probar sus controles de seguridad de la información y sus respuestas a escenarios que puedan causar una amenaza a sus operaciones.
- Proporcionar los recursos adecuados a la organización para establecer, mantener y mejorar el entorno de seguridad según sea apropiado para el cambiante panorama de riesgos.
- Invertir en las competencias del personal para llevar a cabo sus tareas y proporcionar al personal la capacitación y la conciencia adecuadas relevantes para su función y la información a la que tienen acceso.
- Garantizar que nuestros proveedores y organizaciones asociadas hagan lo mismo, y que establecen y hacen cumplir los estándares de seguridad a aquellos a quienes transmitimos cualquier información.

6. MARCO NORMATIVO

6.1. DATOS DE CARÁCTER PERSONAL

En el ámbito de los datos de carácter personal, aplica:

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

6.2. ESQUEMA NACIONAL DE SEGURIDAD

En el ámbito del Esquema Nacional de Seguridad, está política está integrada por las siguientes normas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

7. ORGANIZACIÓN DE LA SEGURIDAD

7.1. COMITÉ DE SEGURIDAD

Se ha constituido un Comité de Seguridad de la información cuyas funciones serán las siguientes:

El Secretario del Comité de Seguridad de la Información será el Responsable de Seguridad y tendrá como funciones:

- Convoca las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.
- El Comité de Seguridad de la Información reportará a la Junta de Gobierno.
- El Comité de Seguridad de la Información tendrá las siguientes funciones y responsabilidades:
  - Atender las inquietudes de la Junta de Gobierno.
  - Informar regularmente del estado de la seguridad de la información a la Junta de Gobierno.
  - Promover la mejora continua del sistema de gestión de la seguridad de la información.
  - Elaborar la estrategia de evolución de la Organización 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 los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
  - Elaborar (y revisar regularmente) la Política de Seguridad para que sea aprobada por la Dirección.
  - Aprobar la normativa de seguridad de la información.
  - Coordinar todas las funciones de seguridad de la organización.
  - Velar por el cumplimiento de la normativa legal y sectorial de aplicación.
  - Velar por el alineamiento de las actividades de seguridad a los objetivos de la organización.
  - Coordinar y aprobar, en su caso, las propuestas de proyectos recibidas de los diferentes ámbitos de seguridad, encargándose de gestionar un control y

presentación regular del progreso de los proyectos y anuncio de las posibles desviaciones.

- Recibir las inquietudes en materia de seguridad de la Dirección de la entidad y transmitirlas a los responsables departamentales pertinentes, recabando de ellos las correspondientes respuestas y soluciones que, una vez coordinadas, habrán de ser comunicadas a la Dirección.
- Recabar de los responsables de seguridad departamentales informes regulares del estado de la seguridad de la organización y de los posibles incidentes. Estos informes, se consolidan y se resumen para su comunicación a la Dirección de la entidad.
- Coordinar y dar respuesta a las inquietudes transmitidas a través de los responsables de seguridad departamentales.
- Definir, dentro de la Política de Seguridad Corporativa, la asignación de roles y los criterios para alcanzar las garantías pertinentes en lo relativo a segregación de funciones.
- Elaborar y aprobar 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 Organización 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.
- Aprobar planes de mejora de la seguridad de la información de la Organización. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- 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. 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.

7.2. ROLES: FUNCIONES Y RESPONSABILIDADES

Se detallarán a continuación las funciones de los responsables de la organización:

Responsable de la Información

- Responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- Responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
- Establecer los requisitos de la información en materia de seguridad.
- Determinar y aprobar los niveles de seguridad de la información.
- Aprobar la categorización del sistema con respecto a la información.
- Los que se vayan indicando en los documentos dentro del alcance del ENS.

Responsable del Servicio

- Establecer los requisitos del servicio en materia de seguridad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar la categorización del sistema con respecto a los servicios.
- Los que se vayan indicando en los documentos dentro del alcance del ENS.

Responsable de la Seguridad

Sus funciones serán las siguientes

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la organización.
- Promover la formación y concienciación en materia de seguridad dentro de su ámbito de responsabilidad.
- Aprobar la declaración de aplicabilidad.
- Los que se vayan indicando en los documentos dentro del alcance del ENS.

El Responsable de la Seguridad será el secretario del Comité de Seguridad de la Información, y como tal:

- Convoca las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

Responsable del Sistema

Sus funciones serán las siguientes:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
- Potestad para proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.
- Los que se vayan indicando en los documentos dentro del alcance del ENS.

7.3. PROCEDIMIENTOS DE DESIGNACIÓN

El Responsable de Seguridad será nombrado por el Comité de Seguridad de la Información. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

Igualmente, el resto de los cargos indicados en el apartado anterior será designado por el Comité de Seguridad de la Información mediante acta de reunión.

7.4. POLÍTICA DE SEGURIDAD

Será misión del Comité de Seguridad de la Información la revisión anual de esta Política de Seguridad y la propuesta de revisión o mantenimiento de la misma. La Política será

aprobada por el Director General y difundida para que la conozcan todas las partes afectadas.

8. DATOS DE CARÁCTER PERSONAL

LA EMPRESA trata datos de carácter personal. El Documento de Seguridad al que tendrán acceso sólo las personas autorizadas, recoge los registros de actividad de tratamiento de datos afectados y los responsables correspondientes. Todos los sistemas de información de **LA EMPRESA** se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

9. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. 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 Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

10. DESARROLLO DE LA POLÍTICA

Esta Política de Seguridad complementa las políticas de seguridad de **LA EMPRESA** en diferentes materias. La documentación relativa a la Seguridad de la Información estará clasificada en tres niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel: Política de seguridad.
- Segundo nivel: Normativas y procedimientos de seguridad.
- Tercer nivel: Informes, registros y evidencias electrónicas

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.

La normativa de seguridad estará disponible en una carpeta de ficheros compartidos.

11. OBLIGACIONES DEL PERSONAL

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

Todos los miembros de **LA EMPRESA** atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **LA EMPRESA** en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

12. TERCERAS PARTES

Cuando **LA EMPRESA** preste servicios a otras organizaciones públicas o privadas o maneje información de otras organizaciones públicas o privadas, se les hará partícipes de esta Política de Seguridad, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

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

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