

**MÁSTER UNIVERSITARIO EN SEGURIDAD DE LAS
TECNOLOGÍAS DE LA INFORMACIÓN Y LAS
COMUNICACIONES**

TRABAJO FIN DE MÁSTER

**Plan Director de Seguridad y Plan de
Continuidad de Negocio para la
clínica veterinaria XYZ**

Autores:

Alberto Martínez Sánchez

José Fradejas Ordax

Director del Trabajo Fin de Máster

Marcos Gómez Hidalgo

CURSO 2022-2023

RESUMEN

Este Trabajo Fin de Máster (TFM) consiste en la elaboración de un **Plan Director de Seguridad** (PDS) y un **Plan de Continuidad de Negocio** (PCN) para la clínica veterinaria XYZ.

El objetivo del PDS es identificar y evaluar los riesgos de seguridad asociados con la actividad de la clínica y proponer medidas para prevenir y mitigar los posibles incidentes.

En primer lugar, se realiza un análisis de la normativa aplicable en materia de seguridad y se definen los objetivos del plan. A continuación, se lleva a cabo una evaluación de los riesgos de seguridad, teniendo en cuenta tanto los aspectos físicos como los procedimentales y tecnológicos de la clínica.

A partir de esta evaluación, se propondrá un plan de acción que detalle las medidas necesarias para disminuir la criticidad de los mayores riesgos a los que se encuentra expuesta la organización, tanto preventivas como reactivas. Además, se establecen procedimientos para la gestión de incidentes y se definen los roles y responsabilidades de los diferentes actores implicados en la seguridad de la clínica.

Finalmente, se presenta un plan de implantación del PDS, definiendo una valoración económica de las medidas y un cronograma para la implementación de dicho plan.

En conclusión, el PDS propuesto permitirá a la clínica veterinaria minimizar los riesgos de seguridad y garantizar la protección de la integridad de los clientes, del personal y de los activos de la clínica.

El objetivo del PCN es garantizar la supervivencia y la capacidad operativa de XYZ frente a posibles interrupciones o desastres. Para ello, se identifican y evalúan los riesgos que podrían afectar al negocio y se proponen medidas para asegurar la continuidad de las operaciones.

En primer lugar, se realiza un análisis de la normativa aplicable y se definen los objetivos del PCN. A continuación, se lleva a cabo una evaluación de los riesgos potenciales, considerando tanto los aspectos internos como los externos que podrían afectar al funcionamiento de la organización.

Con base en esta evaluación, se establecerá un plan de acción que detalle las medidas necesarias para mitigar los riesgos identificados y garantizar la continuidad de las

operaciones. Estas medidas pueden incluir la implementación de sistemas de respaldo, la elaboración de planes de comunicación en caso de crisis y la formación del personal en procedimientos de emergencia.

Además, se definen los roles y responsabilidades de los diferentes actores involucrados en la continuidad del negocio y se establecen procedimientos para la gestión de crisis y la recuperación de las operaciones.

Por último, se presenta un plan de implementación del PCN, que incluye una evaluación económica de las medidas propuestas y un cronograma para su implementación.

En conclusión, el PCN propuesto permitirá a la organización enfrentar y superar posibles interrupciones o desastres, asegurando la continuidad de las operaciones y protegiendo los activos y la reputación de la empresa.

ABSTRACT

This final Master's Thesis consists of the development of a **Security Master Plan** (SMP) and a **Business Continuity Plan** (BCP) for XYZ Veterinary Clinic.

The objective of the SMP is to identify and assess security risks associated with the clinic's activities and propose measures to prevent and mitigate potential incidents.

Firstly, an analysis of applicable security regulations is conducted, and the plan's objectives are defined. Subsequently, a security risk assessment is carried out, considering both physical and procedural as well as technological aspects of the clinic.

Based on this assessment, an action plan is proposed, detailing the necessary measures to decrease the criticality of the most significant risks faced by the organization, both in terms of preventive and reactive actions. Furthermore, procedures for incident management are established, and roles and responsibilities of different stakeholders involved in the clinic's security are defined. Finally, an implementation plan for the SMP is presented, including an economic evaluation of the measures and a schedule for plan implementation.

In conclusion, the proposed SMP will enable the veterinary clinic to minimize security risks and ensure the protection of the integrity of clients, staff, and clinic assets.

The objective of the BCP is to guarantee the survival and operational capability of XYZ in the face of potential disruptions or disasters. To achieve this, risks that could affect the business are identified and evaluated, and measures are proposed to ensure operational continuity. Firstly, an analysis of applicable regulations is conducted, and the objectives of the BCP are defined. Subsequently, a assessment of potential risks is carried out, considering both internal and external factors that could impact the organization's functioning.

Based on this assessment, an action plan is established, detailing the necessary measures to mitigate identified risks and ensure operational continuity. These measures may include the implementation of backup systems, development of crisis communication plans, and staff training in emergency procedures. Additionally, roles and responsibilities of various stakeholders involved in business continuity are defined, and procedures for crisis management and operational recovery are established.

Finally, an implementation plan for the BCP is presented, including an economic evaluation of proposed measures and a timeline for plan implementation.

In conclusion, the proposed BCP will allow the organization to face and overcome potential disruptions or disasters, ensuring operational continuity and safeguarding assets and the company's reputation.

AGRADECIMIENTOS

Queremos expresar nuestro más profundo agradecimiento a todas las personas que han sido parte fundamental en nuestro camino hacia la culminación de este TFM.

En primer lugar, queremos agradecer a los profesores y a la Universidad Europea de Madrid por su dedicación y apoyo en nuestra formación académica. Su experiencia y guía han sido invaluables en nuestro crecimiento tanto profesional como personal, y estamos agradecidos por todas las oportunidades de aprendizaje que se nos ha brindado.

Un agradecimiento especial a nuestro tutor, cuya paciencia, orientación y sabios consejos fueron fundamentales para superar los desafíos iniciales y lograr que este trabajo tomara forma.

También queremos agradecer a nuestra familia por su comprensión y apoyo incondicional durante este tiempo, ya que hemos tenido que sacrificar momentos valiosos para estar inmersos en este proyecto, y su paciencia y aliento nos han dado la fuerza para seguir adelante.

A nuestros amigos, queremos agradecerles por entender que la dedicación a este TFM significó verlos menos y estar presente en menos ocasiones. A pesar de ello, siempre han estado ahí para animarnos y celebrar cada pequeño avance en este camino académico.

Y como no, también deseamos expresar nuestro agradecimiento a nuestras adorables mascotas, esos compañeros peludos que han estado siempre presentes durante nuestras largas sesiones de TFM. Su cariño y lealtad nos han brindado un alivio reconfortante en momentos de tensión y estrés, recordándonos la necesidad de tomarnos pequeños descansos para recargar energías.

Cada una de estas personas han sido un pilar fundamental en este logro, y sin su apoyo y comprensión, no habría sido posible completar este TFM con éxito.

Gracias a todos, profesores, tutor, universidad, familia, amigos y mascotas, por ser parte de este capítulo tan significativo en nuestra trayectoria académica.

Contenido

1.	Introducción	14
1.1.	Objetivos y Alcance	14
2.	Estado del arte	16
2.1.	Sistema de Gestión de la Seguridad de la Información.....	18
2.2.	MAGERIT y PILAR.....	20
2.3.	PDS	20
2.4.	Seguridad en clínicas veterinarias	22
2.5.	Normativa y regulaciones aplicables en materia de seguridad en clínicas veterinarias 24	
2.6.	PCN.....	26
3.	Metodología de trabajo	28
3.1.	Entendimiento de la entidad y su entorno IT.....	29
3.2.	Entendimiento de la función de seguridad de la información de la organización.....	32
4.	Análisis de riesgos	37
4.1.	Identificación de los activos	37
4.2.	Diagrama de dependencias.....	43
4.3.	Valoración de los activos.....	45
4.4.	Evaluación de amenazas	50
4.5.	Determinación del impacto y la probabilidad.....	51
5.	Medidas de seguridad	56
5.1.	Descripción de las medidas de seguridad adoptadas para minimizar los riesgos identificados.....	56
6.	PDS	67
6.1.	Clasificación de los controles según su criticidad	67
6.2.	Plan de Seguridad.....	68
6.2.1.	Definición de medidas específicas a implementar para cada control	69
6.2.2.	Establecimiento de un calendario de implantación.....	72
6.2.3.	Seguimiento y revisión periódica del progreso.....	74
6.2.4.	Evolución de los indicadores de impacto y riesgo.....	75
7.	PCN	78
7.1.	Propósito	79
7.2.	Alcance y Prioridades a la hora de recuperar las funciones críticas	79
7.3.	Centro de Gestión de Emergencias	81
7.4.	Lista de contactos del equipo PCN	81
7.4.1.	Matriz de responsabilidades del equipo de PCN y sustitutos.....	82

7.5.	Procesos de Negocio	83
7.5.1.	Proceso de Negocio “Atención Veterinaria”	83
7.5.1.1.	Formulario de análisis de daños.....	83
7.5.1.2.	Protección de la función de negocio	84
7.5.1.3.	Estrategia de recuperación de la función de negocio	84
7.5.2.	Proceso de Negocio “Gestión de registros veterinarios”	86
7.5.2.1.	Formulario de análisis de daños.....	87
7.5.2.2.	Protección de la función de negocio	88
7.5.2.3.	Estrategia de recuperación de la función de negocio	88
7.5.3.	Proceso de Negocio “Comunicación con clientes”	89
7.5.3.1.	Formulario de análisis de daños.....	90
7.5.3.2.	Protección de la función de negocio	91
7.5.3.3.	Estrategia de recuperación de la función de negocio	91
7.5.4.	Proceso de Negocio “Gestión de inventarios”	92
7.5.4.1.	Formulario de análisis de daños.....	93
7.5.4.2.	Protección de la función de negocio	93
7.5.4.3.	Estrategia de recuperación de la función de negocio	94
7.6.	Análisis del riesgo de los activos	95
7.7.	Gestión de Cambios	100
7.8.	Formación del PCN.....	101
7.9.	Prueba del PCN.....	101
7.10.	Revisión del PCN.....	103
8.	Conclusiones.....	104
8.1.	Resumen de los principales hallazgos del TFM	104
8.2.	Limitaciones del estudio.....	105
8.3.	Recomendaciones para futuros trabajos	105
9.	Acrónimos	106
10.	Índice de Figuras.....	107
11.	Referencias bibliográficas	108
11.1.	Lista de las fuentes consultadas para la elaboración del TFM.....	108
11.2.	Bibliografía	108
12.	Anexos	110
12.1.	Política de la Seguridad de la información	110

1. Introducción

En un entorno cada vez más digitalizado y conectado, la seguridad de la información se ha vuelto crucial para la protección de los datos sensibles de las empresas. En este contexto, la implementación de un PDS se torna imprescindible para impulsar y ayudar a garantizar la confidencialidad, integridad y disponibilidad de la información.

En el ámbito de la salud animal, las clínicas veterinarias gestionan gran cantidad de datos clínicos de sus pacientes, así como información personal de sus dueños, proveedores y entidades externas, así como información financiera y de gestión del negocio. La implementación de un PDS se hace aún más relevante para proteger esta información y garantizar el correcto funcionamiento de los diferentes procesos de negocio.

En este TFM, se abordará la elaboración de un PDS para un caso de uso específico y real, la clínica veterinaria XYZ, con el objetivo de establecer un marco de actuación que permita identificar los riesgos y establecer medidas de prevención y respuesta ante posibles incidentes de seguridad de la información. Se analizarán los aspectos más relevantes de la normativa en materia de protección de datos y seguridad de la información, así como las mejores prácticas y estándares internacionales en la materia.

El desarrollo del trabajo se apoyará en gran medida en los conocimientos y aprendizajes desarrollados durante el máster, e investigando en mayor profundidad áreas de conocimientos como el análisis de riesgos, los sistemas de gestión de seguridad de la información, los planes directores de seguridad o la seguridad en las operaciones, también abordados en el máster.

1.1. Objetivos y Alcance

El principal objetivo del presente TFM es la elaboración de un PDS para la organización XYZ, de manera que se identifiquen los riesgos de seguridad más relevantes a los que se encuentra expuesta la organización, y se establezca un plan a corto y medio plazo para gestionar estos riesgos y mitigarlos hasta un nivel aceptable, preparando así a la empresa y su gestión de la seguridad a unos niveles adecuados pero también a próximos pasos tras el análisis de riesgos y el plan director, que podrían derivar en un futuro en un SGSI, un

PCN, etc. Algunas de estas piezas esenciales se desarrollarán en el contenido y resultados del TFM, otras podrán quedar establecidas en un plan de trabajo a futuro.

Para ello, se realizará un entendimiento de la organización, sus procesos de negocio y su entorno de IT, se identificarán sus diferentes dependencias, incluyendo relaciones con terceros, la propia clientela de la clínica, los proveedores y cadena de suministro, etc. Se realizará un análisis de riesgos para la organización, y se propondrá un plan de acción que detalle las medidas necesarias para disminuir la criticidad de los mayores riesgos a los que se encuentra expuesta la organización, definiendo un presupuesto y un cronograma para la implementación de dicho plan. También se diseñará la política de seguridad de la información de la organización.

Adicionalmente, se desarrollará un PCN, donde se diseñarán e implementarán los pasos a seguir para la recuperación del negocio en caso de un incidente grave de seguridad o contingencias que pongan en riesgo la continuidad de la compañía.

2. Estado del arte

Tal y como se desprende del informe Global Cybersecurity Outlook 2023 del World Economic Forum, la preocupación en ciberseguridad va en aumento tanto por la parte de los responsables de seguridad de las organizaciones como los responsables de negocio. En 2023, un 10% de los responsables de negocio reconocen que no disponen de las personas y recursos necesarios para gestionar los ciberriesgos de su organización, frente al 0% de 2022. La situación geopolítica, las nuevas tecnologías (y por ende las nuevas amenazas) y las diferentes regulaciones relacionadas con la ciberseguridad están obligando a las empresas a fortalecer sus estrategias para la gestión de sus ciberriesgos¹.

El informe “Balance ciberseguridad 2022” de INCIBE, indica que durante el año 2022 atendieron más de 118.820 incidentes, lo que supone un aumento de más de un 8.8% con respecto al año 2021. De estos, un 52% se relacionaban con empresas. Estos datos nos muestran que se están produciendo un aumento significativo en la cantidad de ciberataques, por lo que implementar políticas de buen gobierno y gestión del riesgo es primordial para intentar prevenir que los ataques puedan tener éxito².

El panorama de ciberataques y amenazas cibernéticas a nivel mundial ha experimentado un crecimiento significativo en los últimos años. En un mundo cada vez más digitalizado, los ciberdelincuentes han aprovechado las vulnerabilidades en los sistemas informáticos para llevar a cabo una amplia gama de ataques y actividades maliciosas. Estos ataques representan una seria amenaza para la seguridad de la información, tanto para organizaciones como para individuos. En términos generales, los ciberataques se han vuelto más sofisticados y persistentes. Los actores maliciosos utilizan diversas técnicas para infiltrarse en sistemas y redes.

En este sentido, muchas organizaciones están realizando inversiones moderadamente elevadas en Ciberseguridad, siendo muy recomendable implementar un PDS que ayude a garantizar que la gestión del riesgo se realiza de una forma eficiente y alineada con las necesidades del Negocio.

Existe la percepción entre las Pymes y pequeñas empresas de que no son un objetivo para los atacantes, debido principalmente a su tamaño reducido. Sin embargo, los atacantes han puesto a las pequeñas y medianas empresas en su punto de mira, y cada vez más son el objetivo de ciberataques.

De acuerdo con el informe SMALL BUSINESS CYBER SECURITY GUIDE del gobierno de Australia, las mayores amenazas para una empresa pequeña son³:

- **Phishing.** Es un tipo de ataque de ingeniería social que intenta engañar a los usuarios para obtener acceso no autorizado a sistemas de información o a información confidencial.
- **Ransomware.** Tipo de ataque que cifra el sistema de información que infecta, de manera que los usuarios legítimos no pueden hacer eso del mismo ni de la información que contiene. Se suele pedir un pago a la víctima para descifrar los archivos.
- **Malware.** Software malicioso que intenta obtener acceso no autorizado a sistemas de información o a información confidencial.

Adicionalmente, y dada la frecuencia creciente de los incidentes de seguridad, las organizaciones también están invirtiendo en elaborar su PCN, de forma que les permita a seguir operando durante un incidente grave de seguridad, mientras retornan a un estado anterior al incidente.

En el contexto del **mundo veterinario**, el sector no ha sido inmune a las amenazas ciberneticas. Aunque puede parecer menos atractivo para los ciberdelincuentes en comparación con sectores como el financiero o el de la salud, la industria veterinaria maneja una gran cantidad de datos confidenciales, como registros médicos de animales y datos de clientes. Estos datos son valiosos para los ciberdelincuentes, ya sea para extorsionar a los propietarios de las mascotas o para revenderlos en el mercado negro.

Además, también se enfrenta a otros desafíos ciberneticos específicos. Por ejemplo, la creciente adopción de la telemedicina veterinaria y la digitalización de los registros de salud de los animales aumentan el riesgo de exposición de datos sensibles. Asimismo, los dispositivos conectados, como los equipos de diagnóstico o las cámaras de vigilancia, pueden ser vulnerables a intrusiones y ser utilizados como puntos de entrada para acceder a la red de una clínica veterinaria.

Como muestra, sabemos que durante 2022 al menos 700 clínicas veterinarias fueron impactadas en Estados Unidos, Canadá, Australia y Nueva Zelanda por un ataque

Ransomware⁴. En Madrid, España, se ha registrado un incidente de ciberataque en el sector veterinario este año, donde un hacker ha comprometido la seguridad de varias clínicas veterinarias. Durante el ataque, se ha accedido de manera ilegítima a información sensible, con el claro propósito de obtener beneficios económicos⁵.

En respuesta a estas amenazas, es crucial que el sector veterinario implemente medidas de seguridad adecuadas. Esto incluye la adopción de prácticas de seguridad cibernética, como la formación del personal en concienciación sobre seguridad, la implementación de políticas de acceso y control de datos, el uso de soluciones antivirus y firewall actualizadas, y la realización de copias de seguridad periódicas de los datos.

Por último, es importante fomentar la colaboración y compartir información sobre amenazas y ataques cibernéticos en el sector veterinario. Las organizaciones y clínicas veterinarias pueden beneficiarse de la participación en comunidades y grupos de seguridad, donde pueden intercambiar buenas prácticas y estar al tanto de las últimas tendencias y riesgos en materia de ciberseguridad.

En resumen, el panorama de ciberataques y amenazas cibernéticas a nivel mundial es una preocupación creciente. El sector veterinario no está exento de estas amenazas, ya que maneja datos valiosos y se enfrenta a desafíos específicos. Sin embargo, mediante la implementación de medidas de seguridad adecuadas y la colaboración en el sector, es posible mitigar los riesgos y proteger la información confidencial de los pacientes y clientes del mundo veterinario.

2.1. Sistema de Gestión de la Seguridad de la Información

Un Sistema de Gestión de la Seguridad de la Información (en adelante, SGSI) se puede definir como el conjunto de políticas, procedimientos, guías, recursos y actividades gestionadas por una organización para implementar, operar, monitorizar y revisar y mejorar la seguridad de la información, de forma que esta ayude a la organización a alcanzar sus objetivos de negocio⁶.

El diseño e implementación del SGSI de una organización debe realizarse a la medida de la organización, estando este influenciado por el tamaño, estructura, procesos de negocio, objetivos y necesidades de la organización. El SGSI debe reflejar los intereses y requisitos

de seguridad de la información de todos los stakeholders de la organización (empleados, clientes, proveedores, socios, accionistas y otros terceros).

Para establecer un SGSI se sigue el modelo de Deming o PDCA (Plan-Do-Check-Act o Planificar-Hacer-Verificar-Actuar). Se incluye a continuación un resumen de los objetivos a conseguir en cada etapa⁷:

1. **Planificar.** En esta fase se identifica el SGSI. Se define el alcance del SGSI, la política de seguridad, la metodología que se seguirá para realizar la evaluación de riesgos, se establece el inventario de activos, se realiza un análisis de riesgos y se seleccionan los controles que conformarán el SGSI, así como la declaración de aplicabilidad.
2. **Hacer.** En esta etapa se definen e implementan los planes para tratar los riesgos, se implementan los controles que se han seleccionado en la etapa anterior, se realizan las tareas de formación y concienciación y se opera el SGSI.
3. **Verificar.** En este punto, se revisa el SGSI, se miden la eficacia de los controles, se revisan los riesgos residuales y se audita el SGSI.
4. **Actuar.** En esta etapa se implementan las mejoras en el SGSI, así como las acciones correctivas y detectivas cuya necesidad se ha detectado en la fase anterior.

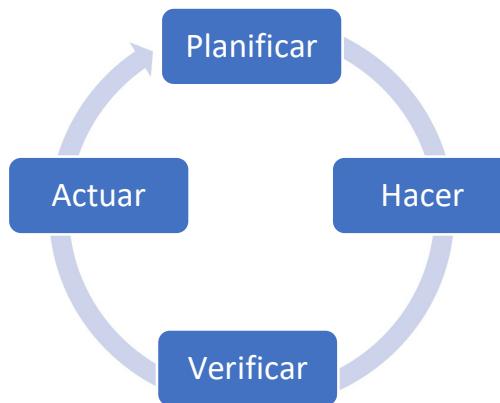


Figura 1: Modelo de Deming o PDCA

Como se muestra en la *Figura 1*, el ciclo de Deming es un proceso recurrente que busca la mejora continua del SGSI.

En resumen, un SGSI busca asegurar que se mantiene la confidencialidad, integridad y disponibilidad de la información, permitiendo a los stakeholders de la organización confiar en que se está realizando una gestión de riesgos adecuada.

2.2. MAGERIT y PILAR

La metodología de análisis y gestión de riesgos de los sistemas de información (en adelante, MAGERIT), es una metodología desarrollada por el Consejo Superior de Administración Electrónica (CSAE) de España. MAGERIT ofrece un método para la realización de análisis y la gestión de riesgos relacionados con los sistemas de información. Mediante esta metodología, se puede estimar el nivel de riesgo de cada activo, a través del análisis de la probabilidad de ocurrencia y el impacto que supondría la materialización de las amenazas existentes sobre los sistemas de información. Como resultado, será posible determinar cuáles son los riesgos más relevantes para la organización, así como establecer un criterio para priorizar las acciones que los mitigan⁸.

Para la realización de este análisis sobre la entidad XYZ de acuerdo con la metodología MAGERIT, vamos a emplear el software PILAR (también llamado Procedimiento Informático-Lógico para el Análisis de Riesgos). Esta herramienta nos permitirá abarcar todas las fases de la metodología MAGERIT: caracterización de los activos, caracterización de las amenazas y evaluación de las salvaguardas.

2.3. PDS

INCIBE define un PDS como “la definición y priorización de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial”⁹. En otras palabras, un PDS engloba las tareas y proyectos relacionados con la seguridad de la información que una organización ha decidido acometer para reducir el nivel de riesgo al que la organización está expuesta hasta un nivel considerado

razonable, entendiendo razonable como el nivel de riesgo que la organización está dispuesta a asumir.

Una vez que la entidad ha establecido la metodología de gestión de riesgos que va a seguir, y ha realizado el primer análisis para identificar la situación en la que se encuentra, el siguiente paso es diseñar planes de acción que mitiguen los riesgos relevantes. Este es precisamente el propósito del PDS, establecer unos objetivos en materia de seguridad de la información que estén alineados con los objetivos de negocio de la empresa, con el fin de reducir los riesgos a los que está expuesta la organización.

La complejidad de un PDS depende de diversos factores, como puede ser el tamaño de la organización, lo tecnológicamente avanzada que sea la misma, el alcance que abarque el PDS, el sector al que pertenece la entidad y las leyes y regulaciones a las que pueda estar sujeta o el tipo de información o datos que maneje. Sin embargo, resulta innegable que para que un PDS tenga éxito este debe incluir una definición clara y acotada de su alcance, así como disponer del apoyo de la Dirección.

A la hora de poner en marcha un PDS, el primer paso consiste en evaluar la situación de la empresa en materia de seguridad de la información. Es decir, es necesario realizar un análisis de contexto de la Organización, del alcance a cubrir y del nivel de control que la entidad ha establecido. También es necesario en este punto entender el contexto de la Organización, así como sus objetivos de negocio. Una vez se dispone de esta información, será necesario realizar un análisis de riesgos para determinar cuáles son las amenazas a las que está expuesta la organización. Llegados a este punto, será posible diseñar planes para contrarrestar estas amenazas, y se establecerán prioridades en función del nivel o valor de cada riesgo (entendiendo valor como la probabilidad del riesgo y su impacto). Finalmente, será necesario que la Dirección apruebe el PDS y realizar revisiones periódicas del mismo para asegurar que se está implantando con éxito, realizando los ajustes que sean necesarios.

Se incluye a continuación una imagen resumen del proceso descrito (*Figura 2*), incluida en el documento PDS de la colección Protege tu empresa de INCIBE.



Figura 2: Proceso del PDS (Fuente INCIBE)

2.4. Seguridad en clínicas veterinarias

La seguridad es un aspecto crucial en la gestión de clínicas veterinarias. Estos establecimientos cuentan con una serie de elementos y áreas críticas que requieren una protección adecuada, desde la gestión de medicamentos hasta la seguridad de las instalaciones y la protección de datos. Por ello, contar con un marco teórico sólido y actualizado resulta fundamental para garantizar una gestión eficiente y efectiva de la seguridad en una clínica veterinaria. En esta sección, se presentarán los conceptos básicos de seguridad en clínicas veterinarias y las normativas y regulaciones aplicables en esta materia, con el objetivo de proporcionar una base sólida para la elaboración de un PDS para XYZ.

- **Definición de seguridad en clínicas veterinarias y su importancia.** La seguridad en clínicas veterinarias se refiere a las medidas y prácticas destinadas a proteger a las personas, los animales, los medicamentos, las instalaciones y la información frente a los riesgos y amenazas a los que están expuestos. La importancia de la seguridad en clínicas veterinarias radica en garantizar la protección y el bienestar de los animales, los trabajadores y los clientes, así como en prevenir incidentes que puedan afectar la continuidad de la clínica. La seguridad también es fundamental para cumplir con las normativas y regulaciones aplicables, y para mantener una buena reputación y confianza en el mercado.
- **Tipos de riesgos y amenazas a los que están expuestas las clínicas veterinarias.** Las clínicas veterinarias están expuestas a una serie de riesgos y amenazas, que pueden ser internos o externos. Entre los riesgos internos se encuentran la gestión inadecuada de medicamentos, la falta de medidas de seguridad en el almacenamiento y dispensación de fármacos, la falta de protección de datos personales y médicos de los clientes, la falta de planes de contingencia ante situaciones de emergencia, y la falta de formación de los trabajadores en seguridad y prevención de riesgos. Por otro lado, entre los riesgos externos se encuentran los robos, los incendios, los accidentes laborales, las situaciones de violencia, los problemas de suministro de energía eléctrica, el acceso no autorizado a las instalaciones, entre otros.
- **Elementos y áreas críticas de seguridad en clínicas veterinarias.** Las clínicas veterinarias cuentan con una serie de elementos y áreas críticas que requieren una protección adecuada:
 - a) Entre estos elementos se encuentran los medicamentos, las historias clínicas, los equipos y utensilios médicos y los instrumentos quirúrgicos.
 - b) Por otro lado, entre las áreas críticas se encuentran las salas de cirugía y procedimientos, las áreas de hospitalización, los almacenes de medicamentos, los cuartos de baño, las salas de espera, y las zonas de atención al cliente. Es fundamental implementar medidas de seguridad específicas en cada una de estas áreas y elementos, para minimizar los riesgos y garantizar la protección adecuada.

- **Métodos y herramientas para la gestión de la seguridad en clínicas veterinarias.** Para garantizar una gestión eficiente y efectiva de la seguridad en clínicas veterinarias, es necesario implementar una serie de métodos y herramientas. Entre estos se encuentran:
 - a) la evaluación de riesgos, que permite identificar y evaluar los riesgos a los que está expuesta la clínica.
 - b) la elaboración de planes de contingencia, que permiten establecer acciones específicas para responder a situaciones de emergencia.
 - c) la formación de empleados, para concienciar a los trabajadores en materia de seguridad de la información.
 - d) la implementación de medidas de seguridad tecnológicas y físicas, para garantizar la protección de la información y las instalaciones.

Además, también se podría contar con un sistema de monitoreo y seguimiento periódico, que permita evaluar y mejorar continuamente las prácticas de seguridad en la clínica.

2.5. Normativa y regulaciones aplicables en materia de seguridad en clínicas veterinarias

En este apartado se abordará la normativa y regulaciones aplicables a las clínicas veterinarias en materia de seguridad en España. Es fundamental conocer y cumplir con las leyes y regulaciones pertinentes para garantizar la protección de la salud y bienestar de los animales, de los propietarios, del personal que trabaja en ellas y de la información.

- **Marco Legal Nacional:** En este punto se analiza la legislación a nivel nacional que tiene relevancia en la seguridad de las clínicas veterinarias. Se mencionan las leyes y reglamentos aplicables y se describe cómo estas normativas establecen las disposiciones generales para la protección de la salud y seguridad en el entorno laboral:
 - a) Ley 31/1995 de Prevención de Riesgos Laborales: Esta ley establece las disposiciones básicas para la protección de la salud y seguridad de los trabajadores en el ámbito laboral. Todas las clínicas veterinarias deben

cumplir con las disposiciones de esta ley para garantizar un entorno seguro para su personal.

- b) Real Decreto 3484/2000 de Protección de los Trabajadores contra los Riesgos relacionados con la Exposición a Agentes Biológicos durante el Trabajo: Este real decreto establece las medidas de protección para los trabajadores expuestos a agentes biológicos, como los veterinarios y el personal de las clínicas veterinarias, que pueden estar en contacto con enfermedades de origen animal.
- c) Real Decreto 53/2013 por el que se establecen las normas básicas aplicables para la protección de los animales utilizados en experimentación y otros fines científicos: Este real decreto establece los requisitos y procedimientos para garantizar el bienestar y la protección de los animales utilizados en experimentación y otros fines científicos. Si una clínica veterinaria lleva a cabo actividades de investigación o experimentación, debe cumplir con esta normativa.
- d) Ley 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, que establece los derechos de los individuos y las obligaciones de las empresas durante los tratamientos de datos considerados personales.
- e) Ley 7/2023, de 28 de marzo, de protección de los derechos y el bienestar de los animales, que tiene como objetivo implementar mecanismos legales con el fin de fomentar la protección animal y prevenir el abandono de animales, estableciendo un marco común en todo el territorio nacional, implicando a los poderes públicos y a la ciudadanía en el respeto de todos los animales, de forma que la tenencia de animales de compañía suponga un compromiso con su cuidado en el transcurso del tiempo, su identificación y su integración en el entorno.

- **Normativa Autonómica de la Comunidad de Madrid:** En este apartado, se aborda la normativa específica aplicable en la Comunidad de Madrid en relación con la seguridad en las clínicas veterinarias:

- a) Ley 2/2006 de Salud de la Comunidad de Madrid: Esta ley regula la salud en la Comunidad de Madrid y establece los requisitos y condiciones sanitarias que deben cumplir los establecimientos sanitarios, incluyendo las clínicas veterinarias. Estos requisitos abarcan aspectos como la higiene y desinfección de las instalaciones, el almacenamiento seguro de medicamentos, el control de plagas y la gestión de residuos.
- b) Decreto 80/1998 por el que se establecen los criterios higiénico-sanitarios y de organización de las consultas y clínicas veterinarias: Este decreto establece los requisitos higiénico-sanitarios y de organización que deben cumplir las clínicas veterinarias en la Comunidad de Madrid. Incluye aspectos como la ubicación y características de las instalaciones, los procedimientos de limpieza y desinfección, la prevención de enfermedades transmisibles y la atención y tratamiento adecuado de los animales.
- c) Ordenanza de Salubridad e Higiene del Ayuntamiento de Madrid: En el caso de las clínicas veterinarias ubicadas en el municipio de Madrid, se deben cumplir las disposiciones establecidas en la Ordenanza de Salubridad e Higiene del Ayuntamiento de Madrid. Esta ordenanza regula aspectos como la prevención y control de enfermedades, la gestión de residuos y la seguridad e higiene en las instalaciones.

2.6. PCN

Podemos definir un Plan de Continuidad de Negocio o PCN como el conjunto de estrategias que ha definido una organización para mitigar los efectos que pueden tener, en caso de materializarse, los riesgos que afectan a los procesos críticos para la entidad¹⁰.

Tal y como recomienda Banco de España en su guía “Recomendaciones relativas a continuidad de negocio”¹¹, la gestión de la continuidad de negocio debería comprender, al menos:

- 1) Análisis del impacto sobre el negocio. También llamado BIA (del inglés, Business Impact Analysis), permite identificar cuáles son las operaciones y servicios críticos para la entidad y los factores (tanto internos como externos) de los que depende la continuidad de estas operaciones y servicios.
- 2) Estrategia de recuperación. A la hora de definir el proceso de recuperación, es necesario establecer unos objetivos y unas prioridades, en función de los resultados del BIA. Adicionalmente, debe incluir los niveles de servicio que la entidad espera mantener para cada proceso crítico de negocio. En concreto:
 - **MTD** (Maximum Tolerable Downtime). Es el periodo máximo que la organización se puede permitir tener una función crítica de negocio sin prestar servicio.
 - **RTO** (Recovery Time Objective). Periodo objetivo que una organización se marca para recuperar una función crítica.
 - **RPO** (Recovery Point Objective). Se define como el punto en el tiempo al que una organización desea recuperar sus datos después de una interrupción, es decir, la cantidad de datos que una organización está dispuesta a perder tras la interrupción y recuperación de un proceso crítico.
- 3) Planes de continuidad de negocio por proceso crítico. Se trata de unas guías para implementar la estrategia de recuperación del proceso crítico evaluado. Establece funciones, responsabilidades y delegación de poderes.
- 4) Pruebas sobre los planes, para verificar su efectividad.
- 5) Programas de comunicación, concienciación y formación.

En resumen, disponer de un PCN es esencial para garantizar la resiliencia y supervivencia de una organización ante situaciones de interrupción o crisis. Ayuda a minimizar las pérdidas, cumplir con los requisitos legales, proteger la reputación, mantener la confianza de los clientes y socios comerciales, y gestionar de manera efectiva los riesgos asociados con la continuidad del negocio.

3. Metodología de trabajo

Se muestran a continuación los pasos seguidos para la elaboración del PDS de la clínica XYZ (*Figura 3*). En primer lugar, se ha realizado un entendimiento de la organización, los procesos de negocio relevantes para la misma y cómo se ha establecido el entorno de IT para apoyar a la organización. Para ello, la metodología seguida se ha basado en entrevistas con los responsables de la organización y visitas a la sede de la misma, para observar la operativa diaria de la organización.

Tras el entendimiento inicial, se ha realizado un análisis del grado de madurez de la función de seguridad de la entidad y una identificación de los activos críticos de la entidad.

Como siguiente paso, se ha realizado un análisis de riesgos sobre los activos críticos que soportan los procesos de negocio de la entidad, realizando una evaluación del impacto y la probabilidad que pueden tener los mismos. Tras el análisis del riesgo inherente, se ha realizado una identificación de los controles que la entidad ha implementado y aquellos controles que se deben implementar para conseguir bajar el nivel de riesgo a un nivel aceptable, considerando el apetito de riesgo de la organización.

Finalmente, con esta información, se ha documentado el PDS de la clínica XYZ.



Figura 3: Pasos elaboración PDS

3.1. Entendimiento de la entidad y su entorno IT

La clínica veterinaria XYZ se encuentra situada en Madrid. El personal de la clínica es muy reducido, contando con una plantilla de 3 veterinarias y un auxiliar veterinario. La clínica ofrece, además de servicios veterinarios, servicios de peluquería canina y felina. Adicionalmente, disponen de una tienda integrada en la clínica con productos para mascotas.

Se puede definir la misión de la clínica XYZ como proporcionar servicios veterinarios integrales, basados en el conocimiento científico y la empatía hacia los animales y sus dueños, ofreciendo un trato personalizado y atención de calidad para garantizar la salud

y el bienestar de las mascotas, mientras que su visión se puede definir como establecerse como una clínica de referencia en el cuidado animal, brindando servicios veterinarios de calidad, promoviendo la salud y el bienestar de las mascotas.

Por último, conviene mencionar los valores de la clínica, los cuales son:

- Ética profesional.
- Compromiso con el cuidado y respeto a los animales
- Honestidad
- Comunicación efectiva

El entorno de la IT de la clínica es relativamente reducido, pero resulta vital para la correcta operación de la organización. Se muestra a continuación el diagrama de red de la organización, en base al entendimiento obtenido en la misma, el cual se describe a continuación (*Figura 4*).

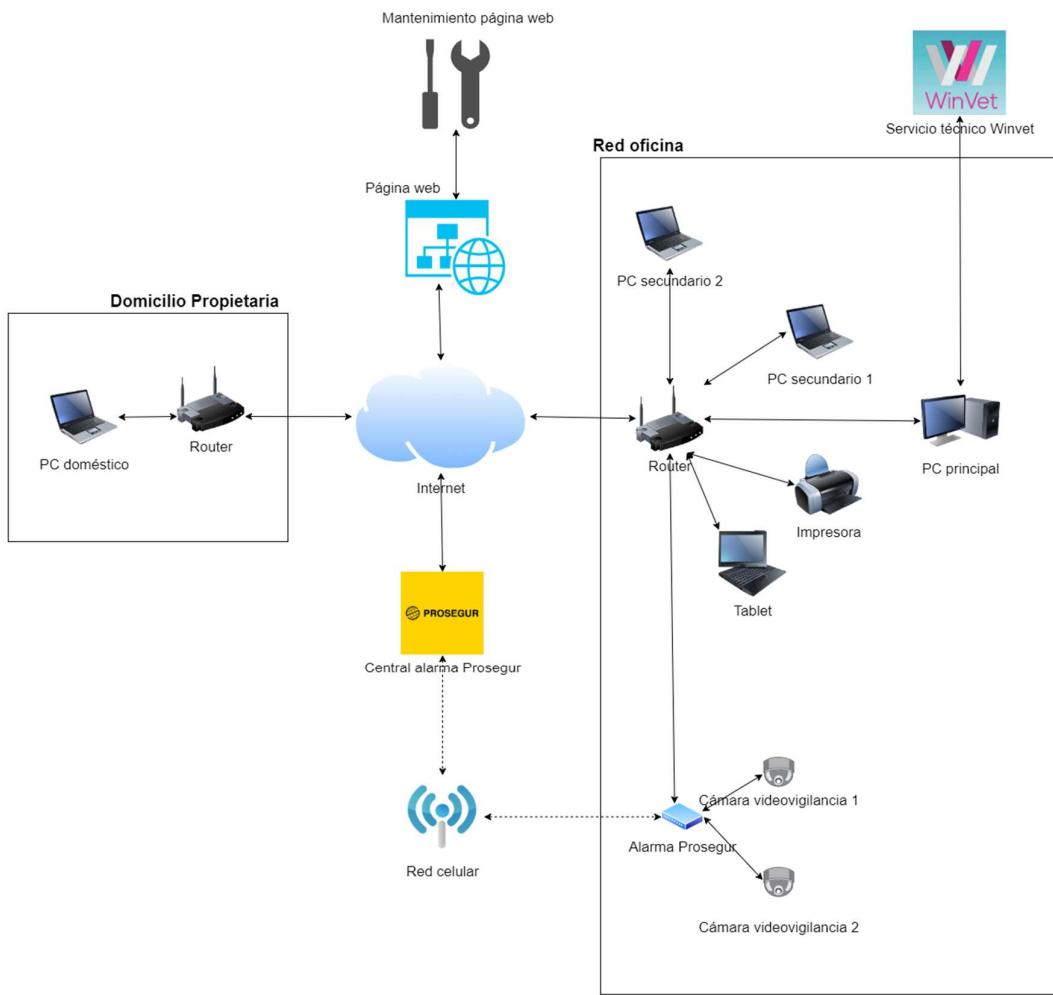


Figura 4: Diagrama de red de XYZ

El grueso de la operativa de negocio está soportado en un aplicativo llamado WINVET. Este aplicativo permite la gestión integral de una clínica veterinaria. La clínica XYZ emplea este aplicativo para los siguientes procesos de negocio:

- Gestión de fichas
- Gestión de citas
- Gestión de expedientes clínicos
- Catálogo (productos y servicios)
- Presupuestos
- Recetas
- Ventas en tienda
- Pagos

- Facturas

El aplicativo, proporcionado por un tercero también llamado Winvet, es un aplicativo instalado en el ordenador principal de la clínica. En este ordenador se almacena tanto el aplicativo como su base de datos, siendo necesario tener este equipo encendido y conectado a la red para que los otros equipos puedan acceder a la aplicación. La entidad tiene también contratado un servicio de mantenimiento con la compañía Winvet, de tal manera que cuando es necesario realizar una actualización o resolver algún incidente, contactan con Winvet, que puede prestar sus servicios tanto de forma remota como presencial.

El proceso de inventario y gestión del stock de la clínica se realiza de forma manual. La entidad cuenta con un catálogo de proveedores de confianza a los que realiza pedidos online, directamente en las plataformas de los vendedores. Si bien el aplicativo WINVET permite la gestión de este proceso, la entidad realizó su análisis y determinó que la gestión manual de este proceso resultaba más eficiente.

El proceso de gestión de nóminas se realiza también de forma manual. Mensualmente, la responsable de la organización realiza el pago de las nóminas accediendo a través de su ordenador personal a su aplicación bancaria.

En lo relativo a la seguridad física, la entidad ha establecido rejas de seguridad en sus dos puertas de entrada. También dispone de cámaras de seguridad en ambas entradas, que forman parte del sistema de alarma que la entidad tiene contratado con Prosegur.

La entidad también dispone de una página web para dar a conocer sus servicios. La página web, basada en wordpress, es puramente informativa. La organización contrató a un desarrollador para la construcción de la web, quien a su vez subcontrató el hosting de la web a Raiola networks.

3.2. Entendimiento de la función de seguridad de la información de la organización

Para lograr un entendimiento de la madurez de la función de seguridad de la información, se han mantenido reuniones con la responsable de la entidad y se ha completado el

checklist disponible en la web de INCIBE¹². Este checklist incluye una serie de controles que toda organización debería incluir en su marco de control interno. Se ha validado el diseño de estos controles con la responsable de la organización para completar el entendimiento sobre la organización e identificar posibles activos.

Identificador	Aspecto a evaluar	Respuesta
<i>Ent_0001</i>	¿La organización ha definido un documento con la política de seguridad de la información?	La entidad no cuenta con una política de seguridad de la información formalmente documentada.
<i>Ent_0002</i>	¿La política de seguridad de la información se revisa periódicamente?	N/A- no se dispone de una política de seguridad de la información
<i>Ent_0003</i>	¿Se han definido las responsabilidades en materia de seguridad de la información?	Las decisiones en materia de seguridad las toma la responsable de la organización.
<i>Ent_0004</i>	¿Existe un Comité de Seguridad encargado de la gestión de los temas relativos a la seguridad de la información?	Debido al tamaño tan reducido de la organización, no existe un comité de Seguridad. Las decisiones en materia de seguridad las toma la responsable de la organización.
<i>Ent_0005</i>	¿Los contratos y acuerdos con terceras partes tienen en consideración los requisitos de seguridad de la organización? (Confidencialidad, propiedad intelectual, etc.).	Se incluyen cláusulas de protección de datos en los contratos con terceras partes.
<i>Ent_0006</i>	¿Se dispone de un inventario de activos?	No se dispone de un inventario de activos formal.
<i>Ent_0007</i>	¿Se ha definido quien es el responsable de los activos?	La responsable de la organización es la responsable de los activos.
<i>Ent_0008</i>	¿Se comprueban las referencias de todos los candidatos a empleo?	N/A- Se trata de una pyme. La responsable de la organización realiza personalmente las entrevistas.

Identificador	Aspecto a evaluar	Respuesta
<i>Ent_0009</i>	¿Se han implantado perímetros de seguridad (paredes, puestos de recepción, entradas controladas por tarjeta) para proteger las áreas de acceso restringido?	Se dispone de un puesto de recepción para impedir el acceso a áreas de acceso restringido.
<i>Ent_0010</i>	¿Los equipos TIC críticos de la organización están ubicados en salas de CPD?	No se dispone de un CPD dedicado. El hosting de la página web está externalizado. Raiola networks presta servicios de hosting. En la clínica se mantiene el SAI en el quirófano.
<i>Ent_0011</i>	¿Se han definido y documentado los procedimientos operacionales TIC?	No se dispone de documentación formal sobre los procedimientos operacionales TIC.
<i>Ent_0012</i>	¿Las copias de seguridad se realizan regularmente de acuerdo con la política de backup establecida?	Se realizan copias de seguridad sobre la base de datos de WINVET, localmente de forma diaria y en un disco duro externo semanalmente. Es un procedimiento manual.
<i>Ent_0013</i>	¿Se verifica regularmente la correcta realización de las copias de seguridad?	No se realizan verificaciones sobre la correcta realización de las copias de seguridad.
<i>Ent_0014</i>	¿Se monitoriza y registra la actividad y el estado de los equipos críticos TIC?	No se realiza una monitorización activa de los equipos críticos. La entidad requiere de estos equipos para operar por lo que un problema en cualquiera de ellos sería rápidamente detectado.
<i>Ent_0015</i>	¿Se registran las actividades de los administradores y operadores de sistema?	El aplicativo que soporta los procesos de negocio de la clínica dispone de logs.
<i>Ent_0016</i>	¿Se ha definido una sistemática para la asignación y uso de privilegios en el sistema?	Se han definido dos tipos de perfiles en los sistemas. La responsable de la organización, y una persona designada como backup, que tienen un perfil con el mayor nivel de privilegio, y el resto de personal, que tiene un perfil con permisos restringidos.

Identificador	Aspecto a evaluar	Respuesta
<i>Ent_0017</i>	¿Se ha definido, documentado e implantado un proceso formal para la asignación de contraseñas?	No se dispone de un procedimiento formalmente documentado.
<i>Ent_0018</i>	¿Se exige a los usuarios que sigan buenas prácticas en materia de seguridad en la selección y uso de contraseñas?	Se indica a los usuarios la necesidad de establecer contraseñas seguras de acuerdo a las buenas prácticas conocidas, pero el sistema no establece ninguna obligatoriedad a la hora de establecer contraseñas.
<i>Ent_0019</i>	¿Los usuarios se aseguran de proteger los equipos desatendidos? (Ej. ¿bloqueando o cerrando la sesión?)	Se indica a los empleados que bloquen los equipos cuando no los están usando.
<i>Ent_0020</i>	¿Las cuentas de usuario del sistema son unipersonales o por el contrario existen cuentas genéricas de usuario?	Las cuentas de usuario son unipersonales.
<i>Ent_0021</i>	¿Se controla la instalación de software en sistemas en producción?	Los equipos se emplean únicamente con fines profesionales y durante el horario laboral. Únicamente la responsable de la organización tendría capacidad para instalar software.
<i>Ent_0022</i>	¿Existe un proceso formal para la gestión de las vulnerabilidades técnicas de los sistemas en uso?	No se ha definido un proceso para la gestión de vulnerabilidades.
<i>Ent_0023</i>	¿Se ha definido, documentado e implantado un proceso formal para la gestión de los incidentes de seguridad?	No se ha definido un proceso para la gestión de los incidentes.
<i>Ent_0024</i>	¿Se ha desarrollado un proceso de gestión para la continuidad del negocio?	No se dispone de un proceso de gestión para la continuidad de negocio.
<i>Ent_0025</i>	¿Se han definido, documentado e implantado planes de continuidad de negocio?	N/A- No se dispone de un proceso de gestión para la continuidad de negocio.
<i>Ent_0026</i>	¿Los planes de continuidad de negocio se revisan y prueban formalmente?	N/A- No se dispone de un proceso de gestión para la continuidad de negocio.

Identificador	Aspecto a evaluar	Respuesta
<i>Ent_0027</i>	¿Todos los requisitos relevantes de carácter legal se mantienen identificados?	Si, se conocen los requerimientos legales.
<i>Ent_0028</i>	¿Se han implementado procedimientos para asegurar el cumplimiento de los requisitos relevantes de carácter legal?	Toda la información personal se almacena dentro del aplicativo WINVET. Para acceder a estos datos, es necesario disponer de los mismos (los datos se almacenan localmente) y disponer de la contraseña de la aplicación.
<i>Ent_0029</i>	¿Se han establecido e implantado procedimientos para la protección y privacidad de la información desde un punto de vista legal?	Toda la información personal se almacena dentro del aplicativo WINVET. Para acceder a estos datos, es necesario disponer de los mismos (los datos se almacenan localmente) y disponer de la contraseña de la aplicación.
<i>Ent_0030</i>	¿Se verifican los sistemas de información regularmente para comprobar su adecuación a los estándares de seguridad implementados?	No se realizan revisiones periódicas sobre los sistemas.

4. Análisis de riesgos

En este apartado se identifican los riesgos asociados con la seguridad de la clínica en base a sus activos críticos, evaluando la probabilidad y el impacto de los riesgos sobre estos activos. Esto permite identificar cuáles son los riesgos más críticos a los que está expuesta la entidad, y establecer un criterio para priorizar las acciones de mitigación para reducirlos, mejorando así la seguridad de la clínica y sus activos críticos.

4.1. Identificación de los activos

El primer paso consiste en identificar y enumerar todos los activos relevantes de XYZ. Para ello, se ha visitado la clínica y se han mantenido varias entrevistas con la dirección. Con ello se ha conseguido un entendimiento inicial sobre la organización y se ha construido el inventario de activos de la organización.

Nº	Identificador	Nombre	Descripción	Ubicación	Crítico
1	<i>ROU</i>	Router	Router para el acceso a la red	Consulta 1	No
2	<i>ROUDOM</i>	Router Domicilio	Router para el acceso a la red	Domicilio	No
3	<i>PC1</i>	PC principal	Equipo principal. Ejecuta la aplicación WINVET y contiene la base de datos de la misma	Consulta 1	Sí
4	<i>PC2</i>	PC secundario 1	Equipo secundario para ser usado por otro profesional veterinario	Consulta 2	No
5	<i>PC3</i>	PC secundario 2	Equipo secundario usado en recepción	Recepción	No
6	<i>PC4</i>	PC doméstico	Equipo en el domicilio de la responsable de la empresa	Domicilio personal de la responsable de la empresa	No
7	<i>TABI</i>	Tablet	Tablet	Consulta 1	No

Nº	Identificador	Nombre	Descripción	Ubicación	Crítico
8	TPV	Datáfono	TPV empleado para realizar cobros	Recepción	No
9	TEL	Teléfono	Teléfono de la organización	Recepción	No
10	IMP	Impresora	Impresora de la organización	Recepción	No
11	SAI	SAI	Sistema de alimentación ininterrumpida para alimentar el equipamiento médico imprescindible en caso de un corte del suministro eléctrico	Quirófano	Sí
12	BAT	Batería PC principal	Batería externa para alimentar el equipo principal en caso de corte del suministro eléctrico	Consulta 1	Sí
13	WEB	Página web	Página web de la organización	Cloud	No
14	WIN	Winvet	Aplicación para la gestión de la clínica	Ordenador sobremesa (equipo principal) - Consulta 1	Sí
15	MAT1	Material veterinario	Material veterinario	Almacén	Sí
16	MAT2	Equipamiento veterinario	Equipamiento veterinario	Almacén	Sí
17	ANT	Antivirus	Antivirus	Ordenador sobremesa (equipo principal) - Consulta 1	No
18	DAT1	Información empleados	Información personal de los empleados de la clínica	Ordenador sobremesa (equipo principal) - Consulta 1	Sí
19	DAT2	Información propietarios	Información de los datos personales de los propietarios	Ordenador sobremesa (equipo principal) - Consulta 1	Sí

Nº	Identificador	Nombre	Descripción	Ubicación	Crítico
20	<i>DAT3</i>	Información contable	Información relativa a la facturación	Ordenador sobremesa (equipo principal) - Consulta 1	Sí
21	<i>DAT4</i>	Información pacientes	Información de las mascotas de los propietarios y los tratamientos realizados	Ordenador sobremesa (equipo principal) - Consulta 1	Si
22	<i>DAT NOM</i>	Información de las nóminas	Información de las Nóminas de los empleados	Ordenador sobremesa (PC doméstico)	Si
23	<i>CAMI</i>	Cámara vigilancia 1	Cámaras de videovigilancia	Entrada	No
24	<i>CAM2</i>	Cámara vigilancia 2	Sistema de alarma de Prosegur	Entrada	No
25	<i>ALA</i>	Sistema alarma	Sistema de alarma de Prosegur	Entrada	No
26	<i>DIS</i>	Disco duro externo	Disco duro externo empleado para almacenar semanalmente una copia de seguridad	Domicilio personal de la responsable de la empresa	No
27	<i>PROV1</i>	Proveedor Winvet	Proveedor que presta servicio de mantenimiento del aplicativo WINVET	N/A	No
28	<i>PROV2</i>	Proveedor sistema alarma	Proveedor que presta servicios de alarma	N/A	No
29	<i>PROV3</i>	Proveedor página web	Proveedor que presta servicio de desarrollo y mantenimiento de la página web	N/A	No
30	<i>ISP</i>	Proveedor Internet	Proveedor de servicios de Internet	N/A	No
31	<i>REJI</i>	Reja entrada 1	Reja para proteger la entrada 1	Puerta entrada 1	No

Nº	Identificador	Nombre	Descripción	Ubicación	Crítico
32	REJ2	Reja entrada 2	Reja para proteger la entrada 2	Puerta entrada 2	No
33	OF	Sede clínica	Cílica XYZ (edificio)	N/A	Sí
34	DOM	Domicilio	Domicilio particular (casa)	N/A	No
35	EMP	Empleados	Empleados clínica	N/A	Sí
36	CLI	Clientes	Clientes clínica	N/A	Si
37	MAS	Mascotas	Mascotas clínica	N/A	Si
38	WFI	Red Wifi	Red Wifi de XYZ	N/A	No
39	WFIDOM	Red Wifi Domicilio	Red Wifi del Domicilio	N/A	No
40	PST	Red telefónica	Red Telefónica	N/A	No
41	MOV	Red móvil	Red móvil	N/A	No
42	ELE	Red eléctrica	Red eléctrica	N/A	Sí

Nº	Identificador	Nombre	Descripción	Ubicación	Crítico
43	<i>ELEDOM</i>	Red eléctrica Domicilio	Red eléctrica del Domicilio	N/A	No
44	<i>INT</i>	Internet	Internet	N/A	No

Para realizar el análisis de riesgos, se ha optado por usar la herramienta PILAR, debido principalmente a su enfoque sistemático, evaluación cualitativa, identificación de áreas críticas, facilitación de la comunicación y apoyo en la toma de decisiones informadas, lo que la convierte en una herramienta altamente útil para la realización de este tipo de análisis.

A continuación, se muestra el inventario de activos (*Figura 5*) descrito anteriormente, una vez se ha transpuesto a la herramienta PILAR.



Figura 5: Inventario de Activos

4.2. Diagrama de dependencias

El diagrama de dependencias entre activos es una representación visual que ilustra las relaciones y dependencias entre los diferentes activos de la clínica. Este diagrama proporciona una comprensión acerca de cómo los activos interactúan entre sí y cómo las vulnerabilidades o amenazas pueden afectarlos.

Cada activo se representa como un nodo y las dependencias se muestran mediante conexiones o líneas que indican las relaciones entre ellos. Estas líneas representan una dependencia de "uso" cuando un activo utiliza o depende de otro activo para funcionar correctamente.

El objetivo principal perseguido con este diagrama es permitir la visualización de las interconexiones y dependencias entre los activos, lo que permite identificar cómo un activo afecta a otros y cómo las interrupciones o vulnerabilidades en un activo pueden propagarse a través de las dependencias y afectar la operación general del sistema.

A continuación, se presenta el diagrama de dependencias de los activos de XYZ (*Figura 6*), el cual proporciona una comprensión clara de cómo interactúan los activos y cómo las amenazas o debilidades podrían propagarse a través de estas dependencias. Esto permite identificar los puntos críticos y las áreas de mayor riesgo, lo que a su vez facilita la planificación y aplicación de medidas de seguridad adecuadas para proteger los activos y mitigar los riesgos asociados.

En el caso de XYZ, si se observa el diagrama, los activos críticos serían:

- Sede principal.
- Red Eléctrica.
- Empleados.
- PC Principal.
- Winvet.

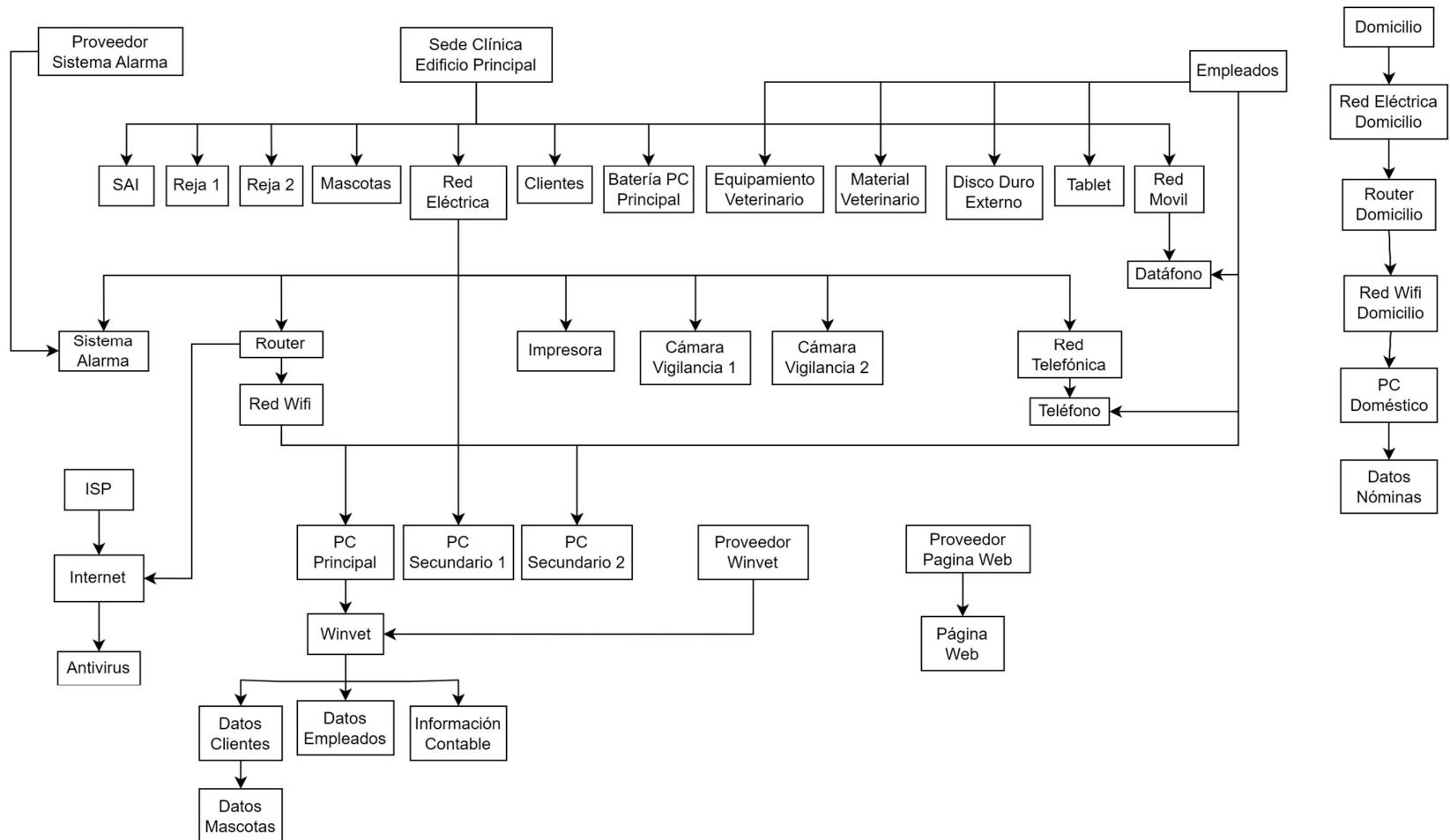


Figura 6: Diagrama de Dependencias

4.3. Valoración de los activos

Una vez identificados los activos, se procede a asignarles un valor en función de su importancia para la clínica. El valor de un activo puede ser determinado por diversos factores, como el costo de adquisición, el tiempo y los recursos invertidos en su desarrollo, su contribución a los ingresos de la organización, su relevancia estratégica...

El valor que se le asigna a cada activo se realiza sobre las diferentes dimensiones que establece PILAR, que son las siguientes:

- **Disponibilidad:** Esta dimensión se refiere a garantizar que los activos de información estén disponibles y accesibles cuando sea necesario, evitando interrupciones o indisponibilidad no autorizada.
- **Integridad:** Esta dimensión se refiere a garantizar la exactitud, completitud y fiabilidad de los activos de información a lo largo de su ciclo de vida, evitando alteraciones o modificaciones no autorizadas.
- **Confidencialidad:** Esta dimensión se refiere a proteger la información de accesos no autorizados, asegurando que solo las personas autorizadas puedan acceder y manejar los activos de información.
- **Autenticidad:** Esta dimensión se refiere al aseguramiento de la identidad u origen de la fuente de los datos.
- **Trazabilidad:** Esta dimensión se refiere a tener la capacidad de rastrear y auditar los eventos y actividades relacionados con los activos de información, lo que permite identificar el origen y las acciones realizadas sobre ellos.
- **Datos Personales:** Esta dimensión se refiere a la protección de los datos personales según las leyes y regulaciones de privacidad aplicables. Incluye garantizar el cumplimiento de los principios de privacidad, obtener el consentimiento adecuado y proteger los derechos de los individuos en relación con sus datos personales.

La siguiente tabla muestra la valoración de los activos de la clínica XYZ:

Grupo	Nombre	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad	Datos Personales
Activos Esenciales	Datos empleados	1	3	5	3	1	5
	Datos propietarios mascotas	5	5	7	5	3	6
	Información contable	1	3	1	3	3	N/A
	Datos Mascotas	5	5	1	3	1	N/A
	Datos Nóminas	1	3	5	3	1	5
	WINVET	7	5	6	5	5	5
Equipamiento	Página web	1	1	0	1	0	N/A
	Antivirus	3	3	1	1	1	N/A
	PC principal	7	5	6	5	3	6
	PC secundario 1	3	5	4	5	3	4
	PC secundario 2	3	5	4	5	3	4
	Tablet	3	3	4	2	1	2
	PC Doméstico	2	3	3	2	2	4
	Datáfono	3	5	3	2	3	0
	Impresora	2	2	4	2	1	4
	Teléfono	4	N/A	1	1	1	N/A
	Disco Duro Externo	5	5	6	5	3	6
	Router	5	2	2	N/A	N/A	N/A
	Red WiFi	5	3	3	1	1	1
	Red WiFi Domicilio	1	1	1	0	0	0
	Red telefónica	3	N/A	1	N/A	N/A	N/A
	Red móvil	3	5	3	N/A	N/A	N/A
	Router Domicilio	1	1	1	N/A	N/A	N/A

Grupo	Nombre	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad	Datos Personales
Instalaciones	Sistema de Alimentación Ininterrumpida	7	N/A	N/A	N/A	N/A	N/A
	Batería PC principal	7	N/A	N/A	N/A	N/A	N/A
	Cámara Vigilancia 1	3	3	N/A	N/A	N/A	4
	Cámara Vigilancia 2	3	3	N/A	N/A	N/A	4
	Sistema Alarma	3	N/A	N/A	N/A	N/A	N/A
	Red Eléctrica	5	N/A	N/A	N/A	N/A	N/A
	Red Eléctrica Domicilio	1	N/A	N/A	N/A	N/A	N/A
	Internet	3	N/A	2	N/A	N/A	1
Usuarios	Sede clínica- Edificio principal	7	N/A	N/A	N/A	N/A	N/A
	Reja para proteger entrada 1	3	N/A	N/A	N/A	N/A	N/A
	Reja para proteger entrada 2	3	N/A	N/A	N/A	N/A	N/A
	Domicilio	1	N/A	N/A	N/A	N/A	N/A
Material	Empleados	7	N/A	N/A	N/A	N/A	N/A
	Clientes	5	N/A	N/A	N/A	N/A	N/A
	Mascotas	5	N/A	N/A	N/A	N/A	N/A
Proveedores	Material veterinario	5	N/A	N/A	N/A	N/A	N/A
	Equipamiento veterinario	5	N/A	N/A	N/A	N/A	N/A
	Proveedor WINVET	5	3	5	5	5	N/A
	Proveedor sistema de alarma	3	N/A	1	1	1	N/A
	Proveedor página web	1	1	1	1	0	1
	ISP	3	N/A	2	N/A	N/A	1

Adicionalmente, se ha realizado el análisis de la valoración de activos teniendo en cuenta las dependencias entre activos que se han establecido en Pilar. Con ello se observa que los activos que dependen de la sede principal de la clínica han adquirido su valor 7 en la disponibilidad ya que dependen directamente de él. A continuación, se muestra la tabla de todos los activos:

Grupo	Nombre	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad	Datos Personales
Activos Esenciales	Datos empleados	7	5	6	5	5	6
	Datos propietarios mascotas	7	5	7	5	5	6
	Información contable	7	5	6	5	5	N/A
	Datos Mascotas	7	5	7	5	5	N/A
	Datos Nóminas	2	3	5	3	2	5
	WINVET	7	5	6	5	5	6
Equipamiento	Página web	1	1	1	1	0	N/A
	Antivirus	3	3	1	1	1	N/A
	PC principal	7	5	6	5	3	6
	PC secundario 1	7	5	4	5	3	4
	PC secundario 2	7	5	4	5	3	4
	Tablet	7	3	4	2	1	2
	PC Doméstico	2	3	3	2	2	4
	Datáfono	7	5	3	2	3	0
	Impresora	7	2	4	2	1	4
	Teléfono	7	N/A	1	1	1	N/A
	Disco Duro Externo	7	5	6	5	3	6
	Router	7	2	2	N/A	N/A	N/A
	Red WiFi	7	3	3	1	1	1
	Red WiFi Domicilio	1	1	1	0	0	0

Grupo	Nombre	Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad	Datos Personales
Equipos	Red telefónica	7	N/A	1	N/A	N/A	N/A
	Red móvil	7	5	3	N/A	N/A	N/A
	Router Domicilio	1	1	1	N/A	N/A	N/A
	Sistema de Alimentación Ininterrumpida	7	N/A	N/A	N/A	N/A	N/A
	Batería PC principal	7	N/A	N/A	N/A	N/A	N/A
	Cámara Vigilancia 1	7	3	N/A	N/A	N/A	4
	Cámara Vigilancia 2	7	3	N/A	N/A	N/A	4
	Sistema Alarma	7	N/A	N/A	N/A	N/A	N/A
	Red Eléctrica	7	N/A	N/A	N/A	N/A	N/A
	Red Eléctrica Domicilio	1	N/A	N/A	N/A	N/A	N/A
	Internet	7	N/A	2	N/A	N/A	1
Instalaciones	Sede clínica- Edificio principal	7	N/A	N/A	N/A	N/A	N/A
	Reja para proteger entrada 1	7	N/A	N/A	N/A	N/A	N/A
	Reja para proteger entrada 2	7	N/A	N/A	N/A	N/A	N/A
	Domicilio	1	N/A	N/A	N/A	N/A	N/A
Usuarios	Empleados	7	N/A	N/A	N/A	N/A	N/A
	Clientes	5	N/A	N/A	N/A	N/A	N/A
	Mascotas	5	N/A	N/A	N/A	N/A	N/A
Material	Material veterinario	7	N/A	N/A	N/A	N/A	N/A
	Equipamiento veterinario	7	N/A	N/A	N/A	N/A	N/A
Proveedores	Proveedor WINVET	5	3	5	5	5	N/A
	Proveedor sistema de alarma	3	N/A	1	1	1	N/A
	Proveedor página web	1	1	1	1	0	1
	ISP	3	N/A	2	N/A	N/A	1

4.4. Evaluación de amenazas

Toda vez los activos han sido identificados, es necesario realizar una evaluación de las posibles amenazas a las que podrían estar expuestos. Esto implica identificar los eventos o situaciones que podrían poner en peligro los activos.

Siendo difícil, por no decir imposible, caracterizar lo que podría ocurrir con los activos en ausencia de unas salvaguardas mínimas ya implementadas, se recurre a una calificación estándar de las amenazas típicas sobre los activos teniendo en cuenta su naturaleza y su valor. Con todas estas consideraciones, la siguiente tabla (*Figura 7*) muestra las amenazas que se han considerado típicas para los activos de la clínica:

activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS								
⌚ [B] Activos esenciales								
⌚ [DAT1] Datos Empleados			1%	10%	50%	100%	50%	100%
⚠ [E.15] Alteración de la información	1	1%						
⚠ [E.18] Destrucción de la información	1	1%						
⚠ [E.19] Fugas de información	1			10%				
⚠ [A.5] Suplantación de la identidad	10		10%	50%	100%			
⚠ [A.6] Abuso de privilegios de acceso	10	1%	10%	50%				
⚠ [A.11] Acceso no autorizado	100		10%	50%				
⚠ [A.13] Repudio (negación de actuaciones)	1					50%		
⚠ [PR.g1] 1. No facilitar la información en materia de protección c	10						20%	
⚠ [PR.g2] 2. Tratar datos inadecuados y excesivos para la finalid	10						50%	
⚠ [PR.g3] 3. Carecer de una base jurídica sobre la que se susten	10						50%	
⚠ [PR.g4] 4. Tratar datos personales con una finalidad distinta p	10						90%	
⚠ [PR.g5] 5. No disponer de una estructura organizativa, proces	5						50%	
⚠ [PR.g6] 6. Almacenar los datos por períodos superiores a los	10						50%	
⚠ [PR.g7] 7. Realizar transferencias internacionales a países qu	10						90%	
⚠ [PR.g8] 8. No tramitar o dificultar el ejercicio de los derechos c	10						100%	
⚠ [PR.g9] 9. Resolución indebida del ejercicio de derechos de lo	10						100%	
⚠ [PR.g10] 10. Seleccionar o mantener una relación con un encar	10						90%	
⚠ [PR.g11] 11. Carecer de mecanismos de supervisión y control	10						90%	
⚠ [PR.g12] 12. No registrar la creación, modificación o cancelació	5						50%	
⚠ [PR.g13] 13. No llevar a cabo por parte del responsable del trat	5						50%	
⚠ [PR.g24] 24. Información no actualizada o incorrecta (pe. regis	10						50%	
⚠ [PR.2g] Obtener un consentimiento dudoso, viciado o inválido	10						50%	
⚠ [PR.2m] Accesos no autorizados a datos personales (modifica	10						30%	
⚠ [PR.2n] Accesos no autorizados a datos personales (lectura)	10						80%	
⌚ [it] Datos propietarios mascotas			1%	10%	50%	100%	50%	100%
⚠ [E.15] Alteración de la información	1	1%						
⚠ [E.18] Destrucción de la información	1	1%						
⚠ [E.19] Fugas de información	1			10%				
⚠ [A.5] Suplantación de la identidad	10		10%	50%	100%			
⚠ [A.6] Abuso de privilegios de acceso	10	1%	10%	50%				
⚠ [A.11] Acceso no autorizado	100		10%	50%				
⚠ [A.13] Repudio (negación de actuaciones)	1					50%		
⚠ [PR.g1] 1. No facilitar la información en materia de protección c	10						20%	
⚠ [PR.g2] 2. Tratar datos inadecuados y excesivos para la finalid	10						50%	
⚠ [PR.g3] 3. Carecer de una base jurídica sobre la que se susten	10						50%	
⚠ [PR.g4] 4. Tratar datos personales con una finalidad distinta p	10						90%	

Figura 7: Probabilidad de las amenazas de las dimensiones de los activos

Esta tabla presenta la siguiente información:

- La primera columna muestra las amenazas típicas sobre el activo.
- La segunda columna recoge la frecuencia de ocurrencia expresada como tasa anual (incidencias por año).

- Las demás columnas recogen la degradación del activo expresada como porcentaje de su valor. Hay una columna por dimensión de seguridad.

4.5. Determinación del impacto y la probabilidad

En este paso, es necesario evaluar el impacto potencial de los riesgos identificados. Esto implica comprender las posibles consecuencias negativas en términos de pérdida de activos, interrupción de operaciones, daño a la reputación, pérdida financiera, etc. Cuanto mayor sea el impacto potencial, mayor será la prioridad para abordar ese riesgo.

Además del impacto, es importante evaluar la probabilidad de que ocurran las amenazas identificadas, es decir, cuán posible es la materialización de la amenaza. Para ello es necesario considerar factores como la frecuencia histórica de eventos similares, la presencia de controles de seguridad existentes, etc. La probabilidad se puede expresar en términos cualitativos (baja, media, alta) o cuantitativos (porcentajes).

Sin tener en cuenta las salvaguardas aún, se obtienen las siguientes estimaciones de impacto (*Figura 8*) y riesgo acumulado (*Figura 9*) para los diferentes activos. Las siguientes tablas recogen para cada activo (filas) la estimación de impacto y riesgo en cada dimensión de seguridad (columnas).

- Impacto acumulado:

activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS						
♀ [B] Activos esenciales						
it [DAT1] Datos Empleados	[1]	[2]	[5]	[5]	[4]	[6]
▲ [E-15] Alteración de la información		[0]				
▲ [E-18] Destrucción de la información	[1]					
▲ [E-19] Fugas de información			[3]			
▲ [A-5] Suplantación de la identidad		[2]	[5]	[5]		
▲ [A-6] Abuso de privilegios de acceso	[1]	[2]	[5]			
▲ [A-11] Acceso no autorizado		[2]	[5]			
▲ [A-13] Repudio (negación de actuaciones)				[4]		
▲ [PR-g1] 1. No facilitar la información en materia de protección de					[4]	
▲ [PR-g2] 2. Tratar datos inadecuados y excesivos para la finalidad					[5]	
▲ [PR-g3] 3. Carecer de una base jurídica sobre la que se sustente					[5]	
▲ [PR-g4] 4. Tratar datos personales con una finalidad distinta para					[6]	
▲ [PR-g5] 5. No disponer de una estructura organizativa, procesos					[5]	
▲ [PR-g6] 6. Almacenar los datos por períodos superiores a los ne					[5]	
▲ [PR-g7] 7. Realizar transferencias internacionales a países que n					[6]	
▲ [PR-g8] 8. No tramitar o dificultar el ejercicio de los derechos de					[6]	
▲ [PR-g9] 9. Resolución indebida del ejercicio de derechos de los i					[6]	
▲ [PR-g10] 10. Seleccionar o mantener una relación con un encarga					[6]	
▲ [PR-g11] 11. Carecer de mecanismos de supervisión y control so					[6]	
▲ [PR-g12] 12. No registrar la creación, modificación o cancelación d					[5]	
▲ [PR-g13] 13. No llevar a cabo por parte del responsable del tratam					[5]	
▲ [PR-g24] 24. Información no actualizada o incorrecta (p.e. registro					[5]	
▲ [PR-2g] Obtener un consentimiento dudoso, viciado o inválido pa					[5]	
▲ [PR-2m] Accesos no autorizados a datos personales (modificaci					[4]	
▲ [PR-2n] Accesos no autorizados a datos personales (lectura)					[6]	
♀ [DAT2] Datos propietarios mascotas	[1]	[2]	[6]	[5]	[4]	[6]
▲ [E-15] Alteración de la información		[0]				
▲ [E-18] Destrucción de la información	[1]					
▲ [E-19] Fugas de información			[4]			
▲ [A-5] Suplantación de la identidad		[2]	[6]	[5]		
▲ [A-6] Abuso de privilegios de acceso	[1]	[2]	[6]			
▲ [A-11] Acceso no autorizado		[2]	[6]			
▲ [A-13] Repudio (negación de actuaciones)				[4]		
▲ [PR-g1] 1. No facilitar la información en materia de protección de					[4]	
▲ [PR-g2] 2. Tratar datos inadecuados y excesivos para la finalidad					[5]	

Figura 8: Impacto acumulado

Para el cálculo del impacto acumulado se tiene en cuenta el valor acumulado sobre el activo (visto anteriormente en el punto 4.3) y la degradación causada por la amenaza (visto anteriormente en el punto 4.4).

- Riesgo acumulado:

activo	[0]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS						
♀ [B] Activos esenciales	(5,4)	(4,5)	(6,3)	(4,8)	(3,9)	(5,4)
♂ [DAT1] Datos Empleados	(2,4)	(3,9)	(5,7)	(4,8)	(3,4)	(5,4)
▲ [E-15] Alteración de la información		{0,87}				
▲ [E-18] Destrucción de la información	(1,5)					
▲ [E-19] Fugas de información			(2,7)			
▲ [A-5] Suplantación de la identidad			(3,0)	(4,8)	(4,8)	
▲ [A-6] Abuso de privilegios de acceso	(2,4)	(3,0)	(4,8)			
▲ [A-11] Acceso no autorizado		(3,9)	(5,7)			
▲ [A-13] Repudio (negación de actuaciones)					(3,4)	
▲ [PR-g1] 1. No facilitar la información en materia de protección de						(4,1)
▲ [PR-g2] 2. Tratar datos inadecuados y excesivos para la finalidad						(4,8)
▲ [PR-g3] 3. Carecer de una base jurídico sobre la que se sustente						(4,8)
▲ [PR-g4] 4. Tratar datos personales con una finalidad distinta para						(5,3)
▲ [PR-g5] 5. No disponer de una estructura organizativa, procesos						(4,6)
▲ [PR-g6] 6. Almacenar los datos por períodos superiores a los ne						(4,8)
▲ [PR-g7] 7. Realizar transferencias internacionales a países que n						(5,3)
▲ [PR-g8] 8. No tramitar o dificultar el ejercicio de los derechos de						(5,4)
▲ [PR-g9] 9. Resolución indebida del ejercicio de derechos de los i						(5,4)
▲ [PR-g10] 10. Seleccionar o mantener una relación con un encarga						(5,3)
▲ [PR-g11] 11. Carecer de mecanismos de supervisión y control só						(5,3)
▲ [PR-g12] 12. No registrar la creación, modificación o cancelació						(4,6)
▲ [PR-g13] 13. No llevar a cabo por parte del responsable del tratam						(4,6)
▲ [PR-g24] 24. Información actualizado o incorrecta (pe. registro						(4,8)
▲ [PR-2g] Obtener un consentimiento dudoso, viciado o inválido pa						(4,8)
▲ [PR-2m] Accesos no autorizados a datos personales (modificaci						(4,4)
▲ [PR-2n] Accesos no autorizados a datos personales (lectura)						(5,2)
♂ [DAT2] Datos propietarios mascotas	(2,4)	(3,9)	(6,3)	(4,8)	(3,4)	(5,4)
♂ [DAT3] Información contable	(2,4)	(3,9)	(5,7)	(4,8)	(3,4)	
♂ [DAT4] Datos Mascotas	(2,4)	(3,9)	(6,3)	(4,8)		
♂ [DAT NOM] Datos Nominas	(0,69)	(2,7)	(5,1)	(3,6)	(1,6)	(4,8)
♂ [WIN] Winvet	(5,1)	(3,9)	(5,7)	(4,8)	(3,4)	(5,4)
♀ [E] Equipoamiento	(5,4)	(4,5)	(4,5)	(1,5)		
♂ [WEB] Página Web	(1,5)	(1,5)	(1,9)			
♂ [ANT] Antivirus	(2,7)	(2,7)	(1,9)			
♂ [ROUDOM] Router Domicilio	(1,9)	(0,75)	(1,0)			
♂ [TAB1] Tablet	(5,4)	(0,98)	(2,8)			

Figura 9: Riesgo acumulado

Para el cálculo del riesgo acumulado se incorpora la frecuencia estimada de ocurrencia de la amenaza (visto anteriormente en el punto 4.4).

En las siguientes dos tablas (*Figuras 10 y 11*) se analiza cada activo (superior) valorado en sí mismo (con valor propio) y se hace un seguimiento de aquellos otros activos (inferiores) de los que depende. Cuando las amenazas se materializan sobre los activos inferiores, el perjuicio repercute sobre los superiores.

- Impacto repercutido:

activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS						
o- it [DAT1] Datos Empleados	[1]	[2]	[5]	[5]	[4]	[6]
o- it [DAT2] Datos propietarios mascotas	[1]	[2]	[6]	[5]	[4]	[6]
o- it [DAT3] Información contable	[1]	[2]	[5]	[5]	[4]	
o- I [DATA4] Datos Mascotas	[1]	[2]	[6]	[5]		
o- it [DAT NOM] Datos Nóminas	[0]	[0]	[4]	[3]	[1]	[5]
o- I [WIN] Winvet	[7]	[5]	[6]	[5]	[4]	[6]
o- A [WEB] Página Web	[1]	[1]	[1]			
o- A [ANT] Antivirus	[3]	[3]	[1]			
o- A [ROUDOM] Router Domicilio	[1]	[0]	[0]			
o- A [TAB1] Tablet	[7]	[0]	[3]			
o- A [PC2] PC secundario 1	[7]					
o- A [PC3] PC Secundario 2	[7]	[2]	[3]			
o- A [PC1] PC Principal	[7]	[5]	[6]	[5]	[2]	[6]
o- [D] disponibilidad	[7]					
o- [I] integridad de los datos						
o- [DAT1] Datos Empleados						
▲ [E.15] Alteración de la información						
▲ [A.5] Suplantación de la identidad						
▲ [A.6] Abuso de privilegios de acceso						
▲ [A.11] Acceso no autorizado						
o- [DAT2] Datos propietarios mascotas						
▲ [E.15] Alteración de la información						
▲ [A.5] Suplantación de la identidad						
▲ [A.6] Abuso de privilegios de acceso						
▲ [A.11] Acceso no autorizado						
o- [DAT3] Información contable						
▲ [E.15] Alteración de la información						
▲ [A.5] Suplantación de la identidad						
▲ [A.6] Abuso de privilegios de acceso						
▲ [A.11] Acceso no autorizado						
o- [DAT4] Datos Mascotas						
▲ [E.15] Alteración de la información						
▲ [A.5] Suplantación de la identidad						
▲ [A.6] Abuso de privilegios de acceso						
▲ [A.11] Acceso no autorizado						
o- [WIN] Winvet						

Figura 10: Impacto repercutido

Para el cálculo del impacto repercutido se utiliza el valor propio del activo superior y la degradación causada por la amenaza sobre el activo inferior indicado.

- Riesgo repercutido:

activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS						
o- it [DAT1] Datos Empleados	(2,4)	(3,9)	[5,7]	(4,8)	(3,4)	(5,4)
o- it [DAT2] Datos propietarios mascotas	(2,4)	(3,9)	(6,3)	(4,8)	(3,4)	(5,4)
o- it [DAT3] Información contable	(2,4)	(3,9)	[5,7]	(4,8)	(3,4)	
o- I [DATA4] Datos Mascotas	(2,4)	(3,9)	(6,3)	(4,8)		
o- it [DAT NOM] Datos Nóminas	(0,69)	(2,7)	[5,1]	(3,6)	(1,6)	(4,8)
o- I [WIN] Winvet	[5,1]	(3,9)	[5,7]	(4,8)	(3,4)	(5,4)
o- A [WEB] Página Web	(1,5)	(1,5)	{1,9}			
o- A [ANT] Antivirus	(2,7)	(2,7)	{1,9}			
o- A [ROUDOM] Router Domicilio	(1,9)	(0,75)	{1,0}			
o- A [TAB1] Tablet	(5,4)	(0,98)	(2,8)			
o- A [PC2] PC secundario 1						
o- A [PC3] PC Secundario 2	(5,4)	(2,1)	(2,8)			
o- A [PC1] PC Principal	(5,4)	(3,9)	[5,7]	(4,8)	(2,2)	(5,4)
o- D disponibilidad	(5,4)					
o- [DAT1] Datos Empleados	(2,4)					
o- E [E.18] Destrucción de la información	(1,5)					
o- A [A.6] Abuso de privilegios de acceso	(2,4)					
o- [DAT2] Datos propietarios mascotas	(2,4)					
o- E [E.18] Destrucción de la información	(1,5)					
o- A [A.6] Abuso de privilegios de acceso	(2,4)					
o- [DAT3] Información contable	(2,4)					
o- E [E.18] Destrucción de la información	(1,5)					
o- A [A.6] Abuso de privilegios de acceso	(2,4)					
o- [DATA4] Datos Mascotas	(2,4)					
o- E [E.18] Destrucción de la información	(1,5)					
o- A [A.6] Abuso de privilegios de acceso	(2,4)					
o- [WIN] Winvet	[5,1]					
o- E [E.5.1] Avería de origen lógico	(4,5)					
o- E [E.8] Difusión de software dañino	(3,3)					
o- E [E.18] Destrucción de la información	(1,5)					
o- E [E.20] Vulnerabilidades de los programas (software)	(1,5)					
o- E [E.21] Errores de mantenimiento / actualización de programa	(2,4)					
o- A [A.6] Abuso de privilegios de acceso	(2,4)					
o- E [E.8] Difusión de software dañino	(5,1)					
o- E [E.22] Manipulación de programas	(4,5)					
o- [PC1] PC Principal	(5,4)					

Figura 11: Riesgo repercutido

Para el cálculo del riesgo repercutido se incorpora la frecuencia estimada de ocurrencia de la amenaza sobre el activo inferior indicado.

5. Medidas de seguridad

En esta sección se detallan las medidas específicas adoptadas para mitigar los riesgos identificados y se analiza la efectividad de cada medida de seguridad para determinar si el nivel de madurez establecido es suficiente o si es necesario realizar modificaciones sobre las medidas para reducir aún más el nivel de riesgo residual. De esta forma, se persigue que la clínica y sus activos críticos estén protegidos de manera efectiva y se reduzca al mínimo el riesgo de incidentes de seguridad.

5.1. Descripción de las medidas de seguridad adoptadas para minimizar los riesgos identificados

Para establecer las medidas de seguridad para minimizar los riesgos identificados en la clínica XYZ se ha seguido la norma ISO 27002:2013. Esta norma se basa en un enfoque de mejores prácticas para la seguridad de la información y abarca una amplia gama de controles y medidas de seguridad. Está diseñada para ser utilizada como un marco de referencia por las organizaciones que desean establecer un sistema de gestión de seguridad de la información (SGSI) o mejorar su seguridad existente.

Esta norma es especialmente útil para las organizaciones que buscan establecer y mantener un enfoque sólido de seguridad de la información en sus operaciones. Proporciona una serie de directrices y mejores prácticas reconocidas internacionalmente que pueden ayudar a proteger los activos de información y gestionar los riesgos de seguridad de manera efectiva.

A continuación, se presenta una tabla que incluye todos los controles de la norma ISO 27002:2013, incluyendo los controles que no se recomienda implantar (NO), los controles que ya han sido implementados por la clínica (SI) y aquellos controles que se propone a la dirección de la clínica implementar en un futuro próximo (SI).

Objetivo de control	Subcategoría	Control	Nombre del control	Implementar	Nivel Actual	Nivel Objetivo
Políticas de seguridad de la información	Directrices de gestión de la seguridad de la información	A.5.1.1 A.5.1.2	Políticas para la seguridad de la información Revisión de las políticas para la seguridad de la información	SI NO	L0 N.A.	L3 N.A.
Organización de la seguridad de la información	Organización interna	A.6.1.1 A.6.1.2 A.6.1.3 A.6.1.4 A.6.1.5	Roles y responsabilidades en seguridad de la información Segregación de tareas Contacto con las autoridades Contacto con grupos de interés especial Seguridad de la información en la gestión de proyectos	SI NO NO NO NO	L2 N.A. L0 N.A. N.A.	L2 N.A. L0 N.A. N.A.
	Los dispositivos móviles y el teletrabajo	A.6.2.1 A.6.2.2	Política de dispositivos móviles Teletrabajo	NO NO	N.A. N.A.	N.A. N.A.
Seguridad relativa a los recursos humanos	Antes del empleo	A.7.1.1 A.7.1.2	Investigación de antecedentes Términos y condiciones del empleo	NO SI	N.A. L2	N.A. L2
	Durante el empleo	A.7.2.1 A.7.2.2 A.7.2.3	Responsabilidades de gestión Concienciación, educación y capacitación en seguridad de la información Proceso disciplinario	SI SI SI	L2 L0 L2	L2 L3 L2
	Finalización del empleo o cambio en el puesto de trabajo	A.7.3.1	Responsabilidades ante la finalización o cambio	SI	L2	L2
Gestión de activos	Responsabilidad sobre los activos	A.8.1.1 A.8.1.2 A.8.1.3 A.8.1.4	Inventario de activos Propiedad de los activos Uso aceptable de los activos Devolución de activos	NO NO NO NO	L0 L0 L0 N.A.	L0 L0 L0 N.A.

Objetivo de control	Subcategoría	Control	Nombre del control	Implementar	Nivel Actual	Nivel Objetivo
Control de acceso	Clasificación de la información	A.8.2.1	Clasificación de la información	NO	L0	L0
		A.8.2.2	Etiquetado de la información	NO	L0	L0
		A.8.2.3	Manipulado de la información	NO	L0	L0
	Manipulación de los soportes	A.8.3.1	Gestión de soportes extraíbles	NO	N.A.	N.A.
		A.8.3.2	Eliminación de soportes	NO	N.A.	N.A.
		A.8.3.3	Soportes físicos en tránsito	NO	N.A.	N.A.
	Gestión de acceso de usuario	A.9.1.1	Política de control de acceso	NO	L0	L0
		A.9.1.2	Acceso a las redes y a los servicios de red	NO	L0	L0
		A.9.2.1	Registro y baja de usuario	SI	L2	L2
		A.9.2.2	Provisión de acceso de usuario	NO	L0	L0
		A.9.2.3	Gestión de privilegios de acceso	SI	L2	L2
		A.9.2.4	Gestión de la información secreta de autenticación de los usuarios	NO	L0	L0
	Responsabilidades del usuario	A.9.2.5	Revisión de los derechos de acceso de usuario	NO	L0	L0
		A.9.2.6	Retirada o reasignación de los derechos de acceso	NO	L0	L0
		A.9.3.1	Uso de la información secreta de autenticación	NO	L0	L0
	Control de acceso a sistemas y aplicaciones	A.9.4.1	Restricción del acceso a la información	NO	L0	L0
		A.9.4.2	Procedimientos seguros de inicio de sesión	NO	L0	L0
		A.9.4.3	Sistema de gestión de contraseñas	SI	L3	L3
		A.9.4.4	Uso de utilidades con privilegios del sistema	NO	L0	L0
		A.9.4.5	Control de acceso al código fuente de los programas	NO	N.A.	N.A.
Criptografía	Controles criptográficos	A.10.1.1	Política de uso de los controles criptográficos	NO	N.A.	N.A.
		A.10.1.2	Gestión de claves	NO	N.A.	N.A.

Objetivo de control	Subcategoría	Control	Nombre del control	Implementar	Nivel Actual	Nivel Objetivo
Seguridad física y del entorno	Áreas seguras	A.11.1.1	Perímetro de seguridad física	SI	L3	L3
		A.11.1.2	Controles físicos de entrada	SI	L3	L3
		A.11.1.3	Seguridad de oficinas, despachos y recursos	SI	L3	L3
		A.11.1.4	Protección contra las amenazas externas y ambientales	SI	L3	L3
		A.11.1.5	El trabajo en áreas seguras	NO	N.A.	N.A.
		A.11.1.6	Áreas de carga y descarga	NO	N.A.	N.A.
	Seguridad de los equipos	A.11.2.1	Emplazamiento y protección de equipos	SI	L1	L3
		A.11.2.2	Instalaciones de suministro	SI	L3	L3
		A.11.2.3	Seguridad del cableado	SI	L1	L3
		A.11.2.4	Mantenimiento de los equipos	NO	L0	L0
		A.11.2.5	Retirada de materiales propiedad de la empresa	NO	L0	L0
		A.11.2.6	Seguridad de los equipos fuera de las instalaciones	NO	N.A.	N.A.
		A.11.2.7	Reutilización o eliminación segura de equipos	NO	N.A.	N.A.
		A.11.2.8	Equipo de usuario desatendido	SI	L0	L3
		A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia	SI	L0	L3
Seguridad de las operaciones	Procedimientos y responsabilidades operacionales	A.12.1.1	Documentación de procedimientos operacionales	NO	N.A.	N.A.
		A.12.1.2	Gestión de cambios	NO	N.A.	N.A.
		A.12.1.3	Gestión de capacidades	NO	N.A.	N.A.
		A.12.1.4	Separación de los recursos de desarrollo, prueba y operación	NO	N.A.	N.A.
	Protección contra el software malicioso (<i>malware</i>)	A.12.2.1	Controles contra el código malicioso	SI	L1	L1
	Copias de seguridad	A.12.3.1	Copias de seguridad de la información	SI	L3	L3

Objetivo de control	Subcategoría	Control	Nombre del control	Implementar	Nivel Actual	Nivel Objetivo
Seguridad de las comunicaciones	Registros y supervisión	A.12.4.1	Registro de eventos	NO	L0	L0
		A.12.4.2	Protección de la información del registro	NO	L0	L0
		A.12.4.3	Registros de administración y operación	NO	L0	L0
		A.12.4.4	Sincronización del reloj	NO	L0	L0
	Control del software en explotación	A.12.5.1	Instalación del software en explotación	NO	N.A.	N.A.
		A.12.6.1	Gestión de las vulnerabilidades técnicas	NO	N.A.	N.A.
	Gestión de la vulnerabilidad técnica	A.12.6.2	Restricción en la instalación de software	SI	L0	L3
		A.12.7.1	Controles de auditoría de sistemas de información	NO	L0	L0
	Gestión de la seguridad de las redes	A.13.1.1	Controles de red	NO	N.A.	N.A.
		A.13.1.2	Seguridad de los servicios de red	NO	N.A.	N.A.
		A.13.1.3	Segregación en redes	NO	N.A.	N.A.
	Intercambio de información	A.13.2.1	Políticas y procedimientos de intercambio de información	NO	N.A.	N.A.
		A.13.2.2	Acuerdos de intercambio de información	NO	N.A.	N.A.
		A.13.2.3	Mensajería electrónica	NO	N.A.	N.A.
		A.13.2.4	Acuerdos de confidencialidad o no revelación	NO	N.A.	N.A.
Adquisición, desarrollo y mantenimiento de los sistemas de información	Requisitos de seguridad en los sistemas de información	A.14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	NO	N.A.	N.A.
		A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas	NO	N.A.	N.A.
		A.14.1.3	Protección de las transacciones de servicios de aplicaciones	NO	N.A.	N.A.
		A.14.2.1	Política de desarrollo seguro	NO	N.A.	N.A.
		A.14.2.2	Procedimiento de control de cambios en sistemas	NO	N.A.	N.A.

Objetivo de control	Subcategoría	Control	Nombre del control	Implementar	Nivel Actual	Nivel Objetivo
	Seguridad en el desarrollo y en los procesos de soporte	A.14.2.3 A.14.2.4 A.14.2.5 A.14.2.6 A.14.2.7 A.14.2.8 A.14.2.9	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo Restricciones a los cambios en los paquetes de software Principios de ingeniería de sistemas seguros Entorno de desarrollo seguro Externalización del desarrollo de software Pruebas funcionales de seguridad de sistemas Pruebas de aceptación de sistemas	NO NO NO NO NO NO NO	N.A. N.A. N.A. N.A. N.A. N.A. N.A.	N.A. N.A. N.A. N.A. N.A. N.A. N.A.
	Datos de prueba	A.14.3.1	Protección de los datos de prueba	NO	N.A.	N.A.
Relación con proveedores	Seguridad en las relaciones con proveedores	A.15.1.1	Política de seguridad de la información en las relaciones con los proveedores	SI	L3	L3
		A.15.1.2	Requisitos de seguridad en contratos con terceros	NO	L0	L0
		A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	NO	L0	L0
	Gestión de la provisión de servicios del proveedor	A.15.2.1 A.15.2.2	Control y revisión de la provisión de servicios del proveedor Gestión de cambios en la provisión del servicio del proveedor	NO NO	L0 L0	L0 L0
Gestión de incidentes de seguridad de la información	Gestión de incidentes de seguridad de la información y mejoras	A.16.1.1 A.16.1.2 A.16.1.3 A.16.1.4 A.16.1.5	Responsabilidades y procedimientos Notificación de los eventos de seguridad de la información Notificación de puntos débiles de la seguridad Evaluación y decisión sobre los eventos de seguridad de información Respuesta a incidentes de seguridad de la información	SI SI NO NO NO	L0 L0 L0 L0 L0	L3 L3 L0 L0 L0

Objetivo de control	Subcategoría	Control	Nombre del control	Implementar	Nivel Actual	Nivel Objetivo
		A.16.1.6 A.16.1.7	Aprendizaje de los incidentes de seguridad de la información Recopilación de evidencias	NO NO	L0 L0	L0 L0
Aspectos de seguridad de la información para la gestión de la continuidad de negocio	Continuidad de la seguridad de la información	A.17.1.1 A.17.1.2 A.17.1.3	Planificación de la continuidad de la seguridad de la información Implementar la continuidad de la seguridad de la información Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI SI NO	L0 L0 L0	L3 L3 L0
	Redundancias.	A.17.2.1	Disponibilidad de los recursos de tratamiento de la información	NO	L0	L0
Cumplimiento	Cumplimiento de los requisitos legales y contractuales	A.18.1.1 A.18.1.2 A.18.1.3 A.18.1.4 A.18.1.5	Identificación de la legislación aplicable y de los requisitos contractuales Derechos de Propiedad Intelectual (DPI) Protección de los registros de la organización Protección y privacidad de la información de carácter personal Regulación de los controles criptográficos	SI NO SI SI NO	L0 L0 L0 L0 L0	L3 L0 L3 L3 L0
	Revisiones de la seguridad de la información	A.18.2.1 A.18.2.2 A.18.2.3	Revisión independiente de la seguridad de la información Cumplimiento de las políticas y normas de seguridad Comprobación del cumplimiento técnico	NO NO NO	L0 L0 L0	L0 L0 L0

Sobre los controles que ya se encuentran implantados y los que se recomienda implantar se les ha asignado una valoración, comprendida entre L0 y L5. Esta valoración se realiza usando los niveles de madurez que PILAR utiliza para evaluar salvaguardas y controles:

- **L0 -> Inexistente:** En el nivel L0 de madurez no se han establecido controles o medidas de seguridad de la información. La organización carece de un enfoque sistemático para proteger sus activos de información y está expuesta a riesgos significativos. No existen políticas ni procedimientos específicos para abordar la seguridad de la información.
- **L1 -> Inicial/Ad hoc:** En el nivel L1 de madurez las salvaguardas existen, pero no se gestionan. La organización ha comenzado a implementar controles básicos de seguridad de la información de manera ad hoc. Estos controles son reactivos y no se han integrado completamente en los procesos y operaciones de la organización.
- **L2 -> reproducible, pero intuitivo:** En el nivel L2 de madurez la organización ha establecido controles más estructurados y consistentes. Se han definido políticas y procedimientos básicos de seguridad de la información. Sin embargo, estos controles aún pueden ser intuitivos y no estar completamente documentados.
- **L3 -> proceso definido:** La organización ha establecido un conjunto definido de políticas, procedimientos y controles de seguridad de la información. Estos controles son más formales y están documentados. Existe una clara asignación de responsabilidades y se han integrado en los procesos y operaciones de la organización.
- **L4 -> gestionado y medible:** La organización ha logrado un alto nivel de madurez en la gestión de la seguridad de la información. Los controles implementados se basan en estándares reconocidos y mejores prácticas. Existen métricas y medidas establecidas para evaluar la eficacia de los controles. Se lleva a cabo un monitoreo regular y se toman medidas correctivas cuando sea necesario.
- **L5 -> optimizado:** El nivel L5 de madurez la organización ha alcanzado la optimización de los controles de seguridad de la información. Se ha logrado una madurez excepcional en la gestión de la seguridad. Los procesos de seguridad de la información se han integrado completamente en todas las actividades y decisiones de la organización. Se realizan mejoras continuas y se adoptan nuevas

tecnologías y enfoques para adaptarse a las cambiantes amenazas y desafíos de seguridad.

- **N.A. -> no aplica:** indica que los controles no son relevantes/aplicables a la organización por el tipo de actividad que realiza, su tamaño o su estructura.

Una vez realizada la evaluación de los riesgos de la clínica y teniendo en cuenta sus necesidades, se propone la implementación de los siguientes controles:

- **A.5.1.1 Políticas para la seguridad de la información:** Este control es uno de los más importantes a implementar ya que implica establecer políticas claras y documentadas que aborden la seguridad de la información en la clínica veterinaria. Al implementar este control, se asegura que los empleados estén al tanto de las medidas de seguridad que deben seguir y que exista un marco de referencia para tomar decisiones relacionadas con la seguridad de la información. Se ha definido la política para XYZ en el Anexo 12.1.
- **A.7.2.2 Concienciación, educación y capacitación en seguridad de la información:** La concienciación y la capacitación son fundamentales para garantizar que los empleados comprendan la importancia de la seguridad de la información y sepan cómo actuar adecuadamente para protegerla. Al implementar este control, se proporciona a los empleados la formación necesaria para reconocer y evitar posibles amenazas de seguridad.
- **A.11.2.1 Emplazamiento y protección de equipos:** Al implementar este control, se asegura que los equipos informáticos y otros dispositivos utilizados en la clínica veterinaria estén ubicados en áreas seguras y protegidas. Esto ayuda a prevenir el robo o daño físico de los equipos, así como el acceso no autorizado a la información almacenada en ellos.
- **A.11.2.3 Seguridad del cableado:** La seguridad del cableado es esencial para proteger la infraestructura de red de la clínica veterinaria. Al implementar este control, se asegura de que el cableado esté adecuadamente protegido contra interferencias y manipulaciones no autorizadas, sobre todo de los animales que en algún momento dado puedan dañarlos.

- A.11.2.8 Equipo de usuario desatendido: Este control se refiere a establecer medidas de seguridad para los equipos que puedan quedar desatendidos, como computadoras o dispositivos móviles. Implementar este control implica asegurarse de que los equipos desatendidos estén bloqueados con contraseñas o cerraduras de pantalla para evitar el acceso no autorizado, sobre todo teniendo en cuenta que el ordenador con toda la información sensible es el que se encuentra en la recepción de la clínica y que en ciertos momentos puede quedar desatendido y que personal no autorizado pueda acceder a información confidencial.
- A.11.2.9 Política de puesto de trabajo despejado y pantalla limpia: Este control se refiere a establecer una política que requiera que los empleados mantengan sus puestos de trabajo despejados y sus pantallas limpias. Al implementar este control, se busca evitar que información sensible quede expuesta a miradas no autorizadas y se reducen los riesgos de fuga de información.
- A.12.6.2 Restricción en la instalación de software: Este control implica establecer restricciones en la instalación de software en los equipos de la clínica veterinaria. Se recomienda limitar la instalación de software a aquellos aprobados y de confianza, y así reducir los riesgos de infecciones por malware y se asegura la integridad de los sistemas.
- A.16.1.1 Responsabilidades y procedimientos: Implementar este control implica definir y asignar claramente las responsabilidades de seguridad de la información a los empleados. Al establecer procedimientos y roles claros, se fomenta una gestión eficaz de la seguridad de la información y se asegura que cada empleado sepa qué se espera de ellos en términos de seguridad.
- A.16.1.2 Notificación de los eventos de seguridad de la información: Este control implica establecer un proceso para notificar y gestionar los eventos de seguridad de la información, como incidentes o brechas de seguridad. Al implementarlo, se asegura una respuesta oportuna y adecuada ante los incidentes, minimizando el impacto y facilitando la recuperación.

- A.17.1.1 Planificación de la continuidad de la seguridad de la información: Este control implica desarrollar un plan de continuidad de la seguridad de la información que establezca las medidas a seguir en caso de interrupciones o desastres. Implementar este control asegura que la clínica veterinaria pueda recuperarse rápidamente y mantener la seguridad de la información en situaciones adversas.
- A.17.1.2 Implementar la continuidad de la seguridad de la información: Al implementar la continuidad de la seguridad de la información, se llevan a cabo las acciones planificadas en el plan de continuidad. Esto incluye la realización de copias de seguridad regulares, la disponibilidad de sistemas redundantes y la realización de pruebas periódicas para garantizar la efectividad de las medidas de continuidad.
- A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales: Este control implica identificar las leyes, regulaciones y requisitos contractuales relevantes en materia de seguridad de la información para la clínica veterinaria. Al hacerlo, se asegura el cumplimiento de las obligaciones legales y contractuales relacionadas con la seguridad de la información.
- A.18.1.3 Protección de los registros de la organización: Implementar este control implica establecer medidas para proteger los registros y documentos de la clínica veterinaria que contienen información sensible. Esto incluye el control de acceso, el almacenamiento seguro y la destrucción adecuada de los registros cuando ya no sean necesarios.
- A.18.1.4 Protección y privacidad de la información de carácter personal: Este control se refiere a garantizar la protección y privacidad de la información de carácter personal que maneja la clínica veterinaria. Al implementar este control, se asegura el cumplimiento de las leyes de protección de datos y se establecen medidas para prevenir el acceso no autorizado o la divulgación indebida de información personal.

6. PDS

En esta sección se describe el PDS que se va a establecer de acuerdo con los controles que se ha decidido implantar en la clínica. Para ello, primero se realizará una clasificación de dichos controles de acuerdo con la criticidad del riesgo que mitigan (a mayor criticidad, mayor urgencia o necesidad de implementación), y seguidamente se establecerá el PDS, indicando cómo deberían acometerse (a alto nivel) las acciones propuestas.

6.1. Clasificación de los controles según su criticidad

Una vez se han definido los controles, se han revisado los indicadores de riesgo e impacto obtenidos a través de Pilar y considerando la actividad y tamaño de la clínica XYZ, se han clasificado los controles por niveles de criticidad de implantación:

- **De carácter urgente:** estos controles son necesarios para mitigar riesgos críticos y garantizar la seguridad de la información. Los siguientes controles deben implementarse de forma prioritaria:
 - Política para la seguridad de la información.
 - Concienciación, educación y capacitación en seguridad de la información.
 - Emplazamiento y protección de equipos.
 - Equipo de usuario desatendido.
 - Identificación de la legislación aplicable y de los requisitos contractuales.
 - Protección de los registros de la organización.
 - Protección y privacidad de la información de carácter personal.
- **Controles importantes:** estos controles son importantes para mitigar riesgos significativos y fortalecer la seguridad de la información. Su implementación es prioritaria, y deben planificarse para ser implementados tras la implementación de los controles urgentes. Estos controles son:
 - Seguridad del cableado.
 - Política de puesto de trabajo despejado y pantalla limpia.

- Restricción en la instalación de software.

- **Oportunidades de mejora:** Los siguientes controles se considera que pueden ser implementados a medio/largo plazo con vistas a mejorar la postura en seguridad de la información de la clínica:

- Responsabilidades y procedimientos.
- Notificación de los eventos de seguridad de la información.
- Planificación de la continuidad de la seguridad de la información.
- Implementar la continuidad de la seguridad de la información.

Esta clasificación se basa en la importancia y urgencia relativa de los controles en función de su impacto en la seguridad de la información de la clínica veterinaria XYZ, considerando el análisis de riesgos presentado anteriormente. Los controles clasificados como "de carácter urgente" deben implementarse cuanto antes para minimizar riesgos que se encuentran a un nivel muy elevado y cumplir con las regulaciones aplicables.

Los controles considerados "importantes" también son relevantes y deben ser implementados después de los controles de carácter urgente. Aunque su impacto en la seguridad de la información no es tan crítico como los controles urgentes, aún abordan riesgos significativos y contribuyen al fortalecimiento de la seguridad en la clínica XYZ.

Por último, los controles categorizados como "oportunidades de mejora" son aquellos que pueden abordarse en etapas posteriores del plan de seguridad, una vez que los controles urgentes e importantes se hayan implementado y estén funcionando adecuadamente.

6.2. Plan de Seguridad

El Plan de Seguridad tiene como objetivo establecer las medidas necesarias para garantizar la protección de la información sensible y minimizar los riesgos de seguridad en la clínica veterinaria. Los controles se han clasificado en tres niveles de criticidad: alta, media y baja, según su impacto en la seguridad de la información y la urgencia de su implementación.

Una vez establecidos los controles específicos a implementar para cada nivel de criticidad, es importante desarrollar un Plan de Acción y Seguimiento para asegurar que se lleven a cabo de manera efectiva y se mantenga la seguridad de la información en la clínica veterinaria XYZ.

El desarrollo de este plan constará de las siguientes etapas:

- Definición de medidas específicas a implementar para cada control.
- Establecimiento de un calendario de implantación
- Seguimiento y revisión periódica

6.2.1. Definición de medidas específicas a implementar para cada control

A continuación, se definen las medidas específicas a implementar en cada control identificado en el plan de seguridad.

- **Política para la seguridad de la información:** se desarrolla la política en el Anexo 12.1 de este documento, abordando aspectos fundamentales de la seguridad de la información en la clínica veterinaria. Esta política habrá que distribuirla o hacerla accesible a todos los empleados de la clínica.
- **Concienciación, educación y capacitación en seguridad de la información:** se sugiere llevar a cabo una única charla dirigida a los 4 empleados de la clínica. Durante esta charla, se enfocará en los riesgos asociados a la seguridad de la información y se proporcionarán las mejores prácticas para protegerla. Se considera que esta charla es suficiente para alcanzar los objetivos deseados. No obstante, se recomienda realizar un seguimiento durante las primeras semanas, ya que será una experiencia nueva para los empleados de la clínica. Además, se sugiere realizar esta actividad una vez al año o cuando se incorporen nuevos empleados a la clínica.
- **Emplazamiento y protección de equipos:** se identificarán las áreas seguras para ubicar los equipos críticos, en concreto el PC principal que se encuentra en la recepción de la clínica y el sistema de backup de la información sensible (disco duro externo), de tal forma que se asegure su protección contra accesos no autorizados.

Considerando las medidas de protección de acceso físico ya implementadas en la clínica (cámaras de vigilancia, rejas, sistema de alarma), consideramos que esta acción sería suficiente para conseguir reducir el riesgo a un nivel aceptable.

- **Equipo de usuario desatendido:** sería necesario establecer una política para la gestión de equipos informáticos desatendidos. Este punto es especialmente relevante para el caso del PC Principal, que contiene la información sensible de la clínica y que se encuentra expuesto en la recepción de la clínica XYZ. Se recomienda establecer alguna medida adicional de seguridad sobre este activo, como por ejemplo la configuración de bloqueo automático de sesiones inactivas cuando el tiempo sea superior a 1 minuto.
Adicionalmente, se ha verificado que la política de contraseñas implementada actualmente en la entidad se encuentra alineada con las mejores prácticas (uso de números, mayúsculas, minúsculas y caracteres especiales y caducidad cada 90 días), por lo que la medida de bloqueo automático para las sesiones inactivas se considera suficiente.
- **Identificación de la legislación aplicable y de los requisitos contractuales:** se realizará un análisis exhaustivo de las leyes y regulaciones aplicables a la protección de la información en el ámbito veterinario, así como los requisitos contractuales relacionados con la seguridad de la información. Asegurarse de su cumplimiento estableciendo medidas adecuadas para proteger la información sensible de acuerdo con los requisitos identificados.
Es importante tomar en consideración las notificaciones provenientes del colegio de veterinarios durante el mes de septiembre, ya que estas estarán relacionadas con la reciente ley de Mascotas que fue aprobada en marzo de 2023.
- **Protección de los registros de la organización:** A pesar de que la clínica ya cuenta con medidas para proteger los registros/archivos, se ha detectado que estas no son suficientes para mitigar los riesgos identificados. En concreto, se ha identificado que la entidad realiza copias de seguridad diarias, pero sólo una copia semanal es almacenada fuera del PC Principal. Así, se identifica un punto único de fallo, ya que en caso de que ocurra algún problema con el PC Principal que impida obtener las copias de seguridad, la entidad podría llegar a perder datos de hasta una semana de antigüedad. Tal y como se describe en

el punto 7 (PCN), el valor del RPO debe ser menor. Por ello, se recomienda la realización de las copias de seguridad diarias en un dispositivo adicional o realizarlas en la nube. En cuanto a la gestión de acceso a la información sensible de la organización, también consideramos que el control de concienciación ayuda a conseguir los objetivos perseguidos por este control.

- **Protección y privacidad de la información de carácter personal:** se deben establecer políticas y procedimientos para proteger la información de carácter personal de los clientes y pacientes, asegurando su confidencialidad y cumplimiento de las leyes y regulaciones de privacidad aplicables.
- **Seguridad del cableado:** Este control ya se encuentra implementado en la clínica, pero durante las visitas presenciales se detectaron oportunidades de mejora. En concreto, se detectó que algunos cables se encontraban a ras de suelo, y considerando que el negocio de la organización es una clínica veterinaria, identificamos un riesgo de que las mascotas puedan deteriorar los cables. Por lo tanto, hay que asegurarse de que los cables estén debidamente organizados y fuera del alcance de las mascotas, incluso si solo hay unas pocas. Utiliza protectores de cables o canalizaciones para mantenerlos alejados del suelo y evitar que sean dañados
- **Política de puesto de trabajo despejado y pantalla limpia:** concienciar a los empleados para mantener los puestos de trabajo libres de documentos confidenciales y garantizar que las pantallas, sobre todo la del PC principal, estén protegidas contra miradas no autorizadas usando protectores de pantalla y bloqueo automático.
- **Restricción en la instalación de software:** implementar mecanismos para restringir la instalación de software no autorizado en los equipos de la clínica veterinaria a los empleados, excepto a la dueña de la clínica, minimizando así los riesgos asociados a software malicioso o no autorizado.
- **Responsabilidades y procedimientos:** se deben establecer los roles y las responsabilidades de los empleados en relación con la seguridad de la información. Siendo pocos empleados no haría falta procedimientos documentados para garantizar el cumplimiento de las políticas de seguridad.
- **Notificación de los eventos de seguridad de la información:** se debe establecer un proceso de notificación y gestión de eventos de seguridad (incluyendo la identificación, registro, análisis, respuesta y seguimiento de los

eventos para mitigar su impacto y prevenir futuros incidentes similares) y quien es el responsable que se encargará de ello.

- **Planificación de la continuidad de la seguridad de la información:** desarrollado en el punto 7 (PCN).
- **Implementar la continuidad de la seguridad de la información:** desarrollado en el punto 7 (PCN).

6.2.2. Establecimiento de un calendario de implantación

Una vez definidas las medidas de seguridad a implementar, es necesario elaborar un calendario detallado que establezca los plazos y las fechas límite para cada una de las actividades de implementación. Este calendario se basará en la priorización de las tareas de acuerdo con la criticidad de los controles y los riesgos identificados en el análisis realizado.

También es importante asegurar que el calendario es realista y factible, teniendo en cuenta los recursos disponibles y los posibles desafíos o limitaciones de la clínica XYZ.

Teniendo todo esto en consideración y estableciendo septiembre de 2023 como fecha de comienzo para la implantación de los controles, se ha desarrollado el siguiente cronograma (*Figura 12*):

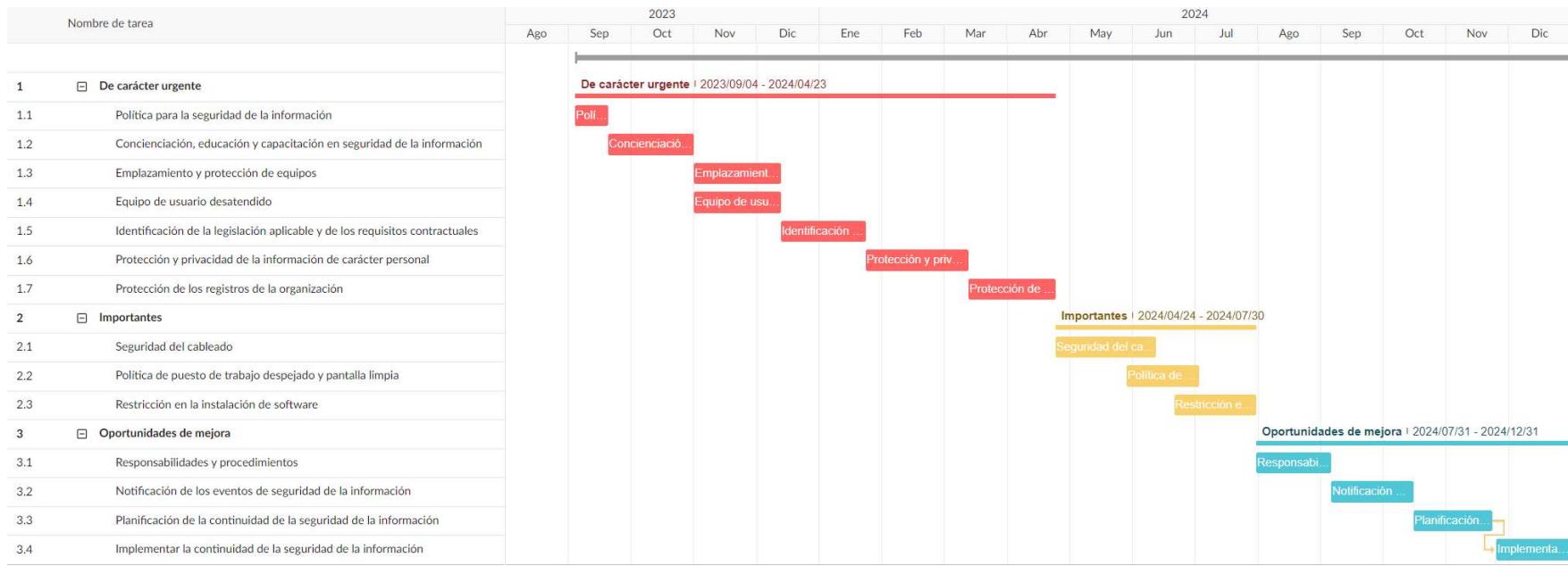


Figura 12: Cronograma

El tiempo total que se ha estimado para la correcta implantación de las medidas de seguridad que la clínica XYZ debe adoptar es de un año y cuatro meses, del 4 de septiembre de 2023 al 31 de diciembre del 2024, dividido en tres bloques que corresponden a los niveles de criticidad establecidos en el punto 6.1:

- Se establece un primer periodo para los controles que se consideran más urgentes, comenzando el 04/09/2023 y terminando el 23/04/2024.
- El segundo periodo, para los controles considerados también importantes, pero no tan urgentes, va del 24/04/2024 al 30/07/2024.
- Por último, el tercer periodo, para el resto de controles que se deberían establecer para terminar de mejorar la seguridad de la clínica, va del 31/07/2024 al 31/12/2024.

6.2.3. Seguimiento y revisión periódica del progreso

Dentro del PDS este apartado es fundamental para garantizar la efectividad y la continuidad de las medidas de seguridad implementadas. Aunque el objetivo de realizar un nuevo análisis de seguridad no esté dentro del alcance del plan, es importante establecer mecanismos de seguimiento y revisión periódica para evaluar el progreso y el rendimiento de las medidas de seguridad implementadas.

El seguimiento y la revisión periódica permiten identificar posibles desviaciones, brechas o debilidades en el sistema de seguridad y tomar las medidas correctivas necesarias. A continuación, se presentan algunos aspectos clave a considerar dentro de este punto:

1. **Establecimiento de indicadores de rendimiento:** se deben definir métricas e indicadores para evaluar el rendimiento de las medidas de seguridad. Estos indicadores pueden incluir el número de incidentes de seguridad, la eficacia de los controles implementados, la detección y respuesta a incidentes... Los indicadores deben ser medibles, relevantes y específicos para poder evaluar de manera adecuada el progreso.
2. **Frecuencia de revisión:** se debe establecer una periodicidad para realizar las revisiones. Esto puede variar según la naturaleza del entorno de seguridad y los riesgos asociados. Por ejemplo, se pueden realizar revisiones trimestrales,

semestrales o anuales, dependiendo de la complejidad y el nivel de riesgo del sistema.

3. **Evaluación de resultados:** durante las revisiones periódicas, se debe evaluar el rendimiento de las medidas de seguridad implementadas. Esto implica comparar los indicadores establecidos con los resultados reales obtenidos. Si se identifican desviaciones o problemas, se deben tomar acciones correctivas para abordar las deficiencias y mejorar la eficacia del sistema de seguridad.
4. **Participación de los responsables de seguridad:** es importante que los responsables de seguridad estén involucrados en el proceso de seguimiento y revisión periódica. Ellos pueden proporcionar información actualizada sobre las amenazas y los riesgos emergentes, así como sugerir mejoras o ajustes necesarios en el plan de seguridad.
5. **Informes de seguimiento:** se deben generar informes periódicos que documenten los resultados de las revisiones y el progreso realizado. Estos informes pueden ser compartidos con la alta dirección y otros interesados relevantes para brindar transparencia y mantenerlos informados sobre el estado de la seguridad.

El seguimiento y la revisión periódica del progreso permiten garantizar que las medidas de seguridad implementadas sean adecuadas y suficientes para proteger los activos y mitigar los riesgos identificados. Aunque no se realice un nuevo análisis de seguridad completo, este punto dentro del PDS brinda la oportunidad de evaluar el rendimiento y realizar ajustes necesarios para mantener la efectividad del sistema de seguridad en el tiempo.

6.2.4. Evolución de los indicadores de impacto y riesgo

Una vez se implanten los controles del plan establecido en el punto 6.2.2, utilizando la herramienta PILAR, se puede ver la evolución del impacto y del riesgo acumulado para cada activo.

Para ello PILAR genera unos informes en modo de gráfico, donde se puede apreciar cómo tanto el impacto como el riesgo sobre los activos de la clínica XYZ disminuirían con la implantación de los controles seleccionados, que se muestran en las *Figuras 13 y 14*:

- Impacto acumulado

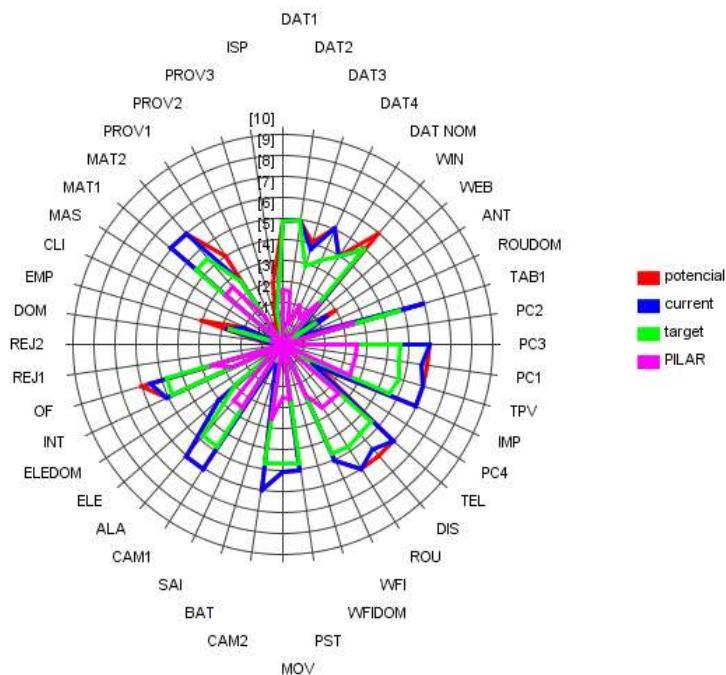


Figura 13: Evolución impacto acumulado

- Riesgo acumulado

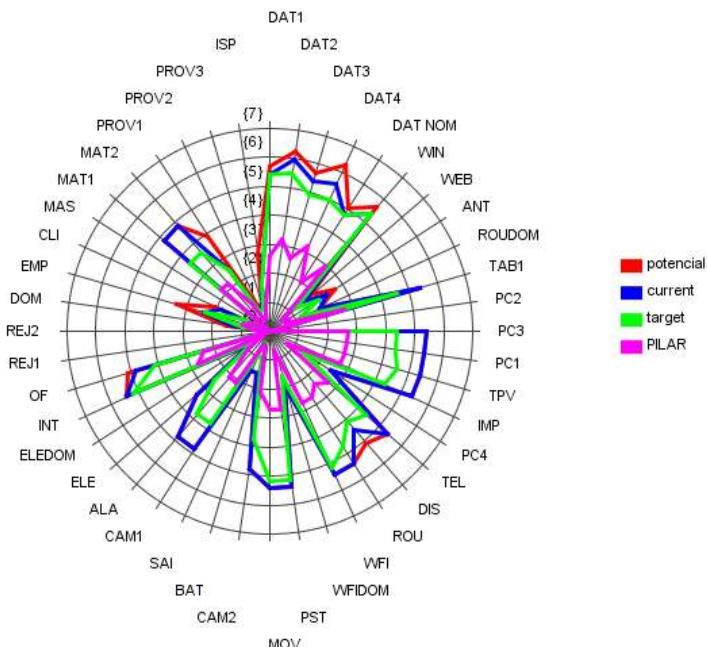


Figura 14: Evolución riesgo acumulado

Leyenda:

- **Potencial**: se muestra el impacto/riesgo de cada activo si no existieran medidas de seguridad en la clínica XYZ.
- **Current**: se muestra el impacto/riesgo de cada activo con los controles que tienen implantados actualmente.
- **Target**: se muestra el impacto/riesgo de cada activo una vez se hayan implantado los controles.
- **PILAR**: sería el hipotético caso de que se siguiera el plan que la herramienta aconseja gracias a toda la información relativa a los valores de cada activo, sus dependencias y amenazas relacionadas.

En estos gráficos se aprecian los cambios positivos en los niveles de riesgo e impacto de los activos gracias a la implementación de salvaguardias en la clínica XYZ. Estos informes revelan cómo las medidas de protección adoptadas han logrado reducir significativamente tanto la probabilidad de incidentes perjudiciales como las consecuencias negativas asociadas a los mismos.

Lo que se pretende con el PDS es demostrar que gracias a la implantación de los controles apropiados los beneficios a corto plazo para la clínica son inmediatos y se reflejan en una disminución inmediata de los riesgos y los impactos negativos. Esto se traduce en una mayor seguridad y estabilidad operativa, lo que a su vez reduce la posibilidad de pérdidas financieras, daños a la reputación e interrupciones en las operaciones. La implementación de salvaguardias también puede conducir a un aumento en la eficiencia de los procesos, ya que se reducen los tiempos de inactividad y se optimiza la utilización de recursos.

A largo plazo, la empresa se beneficia de una mejora continua en su capacidad para prevenir y mitigar riesgos. Al tener en cuenta la evolución de los indicadores de impacto y riesgo a lo largo del tiempo, la empresa puede identificar áreas de mejora, implementar medidas correctivas y fortalecer aún más sus sistemas de protección.

En resumen, los beneficios a corto plazo de la disminución del riesgo y el impacto de los activos incluyen una mayor seguridad operativa, una reducción de pérdidas financieras y una mejora en la eficiencia de los procesos.

7. PCN

Establecer un PCN es fundamental para garantizar la continuidad de las operaciones de negocio durante situaciones de emergencia. En este apartado se describirá el plan de contingencia para hacer frente a situaciones de emergencia y se realizará un análisis del plan de contingencia para asegurar que éste resulta efectivo y se encuentra actualizado.

La clínica XYZ basa su modelo de negocio en la atención de la salud y el bienestar de los animales. Sin embargo, diversos eventos imprevistos, como desastres naturales, fallos en sistemas críticos, incendios o problemas de suministro, pueden interrumpir las operaciones normales de la clínica. Estas interrupciones pueden tener un impacto significativo en la capacidad de brindar atención veterinaria, generar ingresos y mantener la confianza de los clientes.

El PCN es una herramienta vital para gestionar estos riesgos y garantizar que la clínica pueda mantener sus operaciones esenciales, incluso en situaciones adversas. Este plan se basa en una evaluación exhaustiva de los riesgos específicos a los que se enfrenta la clínica veterinaria, y propone una serie de medidas preventivas y de respuesta.

El PCN consta de varios componentes fundamentales, incluyendo:

- **Análisis de riesgos:** En este paso se identifican y evalúan las amenazas potenciales que podrían interrumpir las operaciones de la clínica. Se han analizado en el PDS de la clínica XYZ.
- **Estrategias de mitigación:** Se desarrollan planes y medidas para reducir los riesgos identificados, como la instalación de sistemas de seguridad física, sistemas de respaldo de energía, políticas de seguridad informática, entre otros.
- **Planes de respuesta a emergencias:** Se establecen procedimientos detallados para hacer frente a situaciones de emergencia, incluyendo la activación de un equipo de respuesta, la notificación al personal y a los clientes, y la coordinación con autoridades pertinentes.
- **Planes de recuperación:** Se definen los pasos y acciones necesarios para recuperar las operaciones normales de la clínica una vez que la emergencia haya pasado, incluyendo la reparación de daños, la restauración de sistemas y la comunicación con los clientes, así como la vuelta a la normalidad.

En conjunto, este PCN para XYZ tiene como objetivo principal asegurar la atención continua de los animales y mascotas, mantener la confianza de los clientes y proteger la reputación de la clínica en situaciones adversas.

7.1. Propósito

El propósito del PCN es preparar a la entidad Clínica XYZ para lidiar con los efectos de una emergencia o contingencia que ponga en riesgo la continuidad de los procesos y servicios más críticos, sobre todo aquellos que tienen una mayor dependencia de las tecnologías de la información y las comunicaciones.

Los objetivos del PCN son:

- Definir y priorizar las funciones críticas de negocio, minimizando el impacto en la organización debido a la interrupción de estas.
- Dar respuesta a los riesgos a los que se enfrenta el negocio en caso de interrupciones de sus funciones críticas.
- Detallar la respuesta acordada que dará la Clínica XYZ ante una emergencia.
- Identificar los contactos clave a contactar durante una emergencia.

7.2. Alcance y Prioridades a la hora de recuperar las funciones críticas

Durante el proceso de entendimiento de la compañía, se han mantenido reuniones con la dueña de la clínica XYZ para entender el negocio. Se han identificado aquellos procesos de negocio que resultan claves para la clínica. Así, el PCN de la clínica XYZ, asegura la continuidad de las funciones críticas de negocio descritas en la siguiente tabla.

Función Crítica de Negocio	Causas y motivos de Selección	Prioridad de recuperación (Alta/Media/Baja)
Atención veterinaria	La prestación de servicios veterinarios de calidad y el cuidado de los animales son la razón de ser de la clínica XYZ, constituye la misión de la empresa. No disponer de este servicio tendría graves consecuencias para la clínica, sufriendo esta un elevado coste reputacional.	Alta
Gestión de registros veterinarios	Mantener registros precisos y actualizados de los pacientes es esencial para brindar una atención adecuada y garantizar la continuidad del cuidado. La pérdida o inexactitud de información puede tener consecuencias graves para los animales y la relación con los propietarios.	Alta
Comunicación con clientes	La comunicación efectiva con los propietarios de mascotas es fundamental para el negocio de la clínica, siendo este uno de sus valores. Proporcionar un excelente servicio al cliente, responder a las consultas y preocupaciones de manera efectiva, y establecer relaciones sólidas con ellos son aspectos críticos para mantener la demanda y el crecimiento del negocio.	Media
Gestión de Inventarios	La gestión adecuada del inventario de la clínica resulta esencial para brindar una atención ininterrumpida. La falta de stock o el manejo ineficiente pueden afectar la capacidad de brindar servicios a los pacientes y generar insatisfacción entre los clientes.	Media

Para cada una de las funciones críticas de negocio, se identificarán los activos que juegan un papel en el mismo, se establecerán los valores MTD (máximo tiempo que el proceso puede estar caído), RTO (tiempo objetivo para recuperar el proceso de negocio) y RPO (cantidad de datos que pueden haberse perdido, como máximo).

También se creará el formulario que el responsable del proceso tendrá que completar cuando esté realizando el análisis del incidente, se listarán los controles que la entidad ha establecido para mitigar los riesgos derivados de la falta de disponibilidad de la función de negocio y se listarán también los controles establecidos por la clínica XYZ para conseguir la recuperación del servicio.

7.3. Centro de Gestión de Emergencias

Se detalla a continuación el punto de encuentro para que el equipo de continuidad de negocio (descrito más adelante) pueda realizar sus labores. Se ha definido un sitio primario y un sitio secundario, siendo el secundario el sitio alternativo al que acudir en caso de no estar disponible el sitio primario. Es necesario reiterar que el objetivo del sitio secundario no es proporcionar un espacio alternativo en el que la clínica pueda realizar sus procesos de negocio, sino proporcionar un centro de operaciones físico donde el equipo de continuidad de negocio pueda realizar sus labores.

- **Sitio Primario:** Sede de la clínica XYZ.
- **Sitio Secundario:** Domicilio de la propietaria de la clínica.

Se les entregará a los miembros del equipo de continuidad de negocio las direcciones y los números de teléfono.

7.4. Lista de contactos del equipo PCN

Se incluye a continuación la lista de contactos del equipo de PCN. Por privacidad se han omitido el nombre y el teléfono de los miembros del equipo de continuidad de negocio.

ID	Nombre	Título	Rol	Teléfono
1	***	Dueña clínica	Responsable	***
2	***	Veterinaria	Responsable secundario/sustituto	***
3	***	Proveedor- Servicio técnico WINVET 1	Servicio técnico WINVET 1	***
4	***	Proveedor- Servicio técnico WINVET 2	Servicio técnico WINVET 2	***

7.4.1. Matriz de responsabilidades del equipo de PCN y sustitutos.

En caso de activar el PCN, los miembros del equipo de continuidad de negocio deben asumir sus responsabilidades tan pronto como sea posible. La siguiente tabla muestra el listado de responsabilidades clave, la persona responsable y el suplente designado si la persona responsable no está disponible.

Responsabilidad	Responsable Principal	Suplente
Responsabilidades Operaciones (respuesta a incidentes y recuperación)		
Realizar el triaje del incidente (falsa alarma, amenaza la vida humana, no amenaza la vida humana) y notificarlo al equipo	Responsable	Responsable Secundario
Ordena la evacuación del edificio	Responsable	Responsable Secundario
Realiza un análisis de los daños y proporciona un análisis situacional al equipo de continuidad de negocio	Responsable	Responsable Secundario
Establece los preparativos para la relocalización del personal	Responsable	Responsable Secundario
Responsable recuperación proceso atención veterinaria	Responsable	Responsable Secundario
Responsable recuperación proceso gestión de registros veterinarios	Servicio técnico WINVET 1	Servicio técnico WINVET 2
Responsable recuperación proceso comunicación con clientes	Responsable	Responsable Secundario
Responsable recuperación proceso gestión de Inventarios	Responsable Secundario	Responsable
Responsabilidades tácticas (gestión de incidentes)		
Declarar un incidente de continuidad de negocio e iniciar el PCN	Responsable	Responsable Secundario
Detener el PCN	Responsable	Responsable Secundario
Autorizar y aprobar gastos	Responsable	Responsable Secundario
Ánalisis periódico de la situación y la necesidad de acciones correctivas	Responsable	Responsable Secundario
Coordinación de recuperación: asegurar que el proceso para recuperar las funciones críticas de negocio progresá adecuadamente.	Responsable Secundario	Responsable
Responsabilidades estratégicas		
Planificación y decisión de vuelta a la normalidad	Responsable	Responsable Secundario
Comunicación con los stakeholders	Responsable	Responsable Secundario
Comunicación con la prensa	Responsable	Responsable Secundario

7.5. Procesos de Negocio

7.5.1. Proceso de Negocio “Atención Veterinaria”

El proceso de **Atención Veterinaria** es el proceso principal de la clínica XYZ, y resulta primordial recuperarlo para que la compañía pueda continuar operando. Existe una alta dependencia con el personal veterinario, ya que sin ellos no es posible prestar la atención veterinaria. Adicionalmente, también existen dependencias con el edificio, el material y el equipamiento veterinario, y con el aplicativo Winvet, donde se almacenan los datos de las atenciones veterinarias prestadas (ver proceso de gestión de registros veterinarios).

En caso de un incidente que afecte a este proceso, la máxima prioridad será terminar de realizar aquellas actuaciones que no puedan pararse. El equipo de veterinarios podrá atender (hasta cierto punto) ciertas urgencias de forma manual. Para tratamientos no urgentes, el personal de la clínica redirigirá a los dueños de las mascotas a otro centro veterinario.

De cara a la contención del incidente o emergencia y a la recuperación de los activos, la compañía dispone de un listado con el contacto de los proveedores con los que se tendrá que coordinar para asegurar la recuperación del proceso. Se almacenará una copia del listado en las instalaciones de la organización y otra copia fuera de las instalaciones.

En cuanto al proceso de negocio y la resiliencia de la clínica, se han definido los siguientes valores:

- MTD: 1 semana.
- RPO: 1 día.
- RTO: 2 días.

7.5.1.1. Formulario de análisis de daños

Se incluye a continuación el formulario que tendrá que ser completado por el responsable del proceso de negocio **Atención Veterinaria** en el momento en el que ocurra un incidente. Así, para cada uno de los activos listados en el formulario, el responsable del

proceso tendrá que indicar la gravedad del daño que ha sufrido el activo y cuál es la acción que se sugiere realizar para recuperar el activo (salvar, reparar, recuperar o reemplazar).

Nombre del proceso Atención Veterinaria	Responsable del proceso	Responsable
Activos que soportan el proceso	Daño incurrido (incluyendo evaluador y fecha)	Acción sugerida (Salvar, reparar, recuperar, reemplazar/comprar)
Empleados		
Edificio principal		
Material veterinario		
Equipamiento veterinario		
Winvet		
PC principal		
Red Eléctrica		

7.5.1.2. Protección de la función de negocio

La clínica XYZ dispone de ciertos controles de continuidad, descritos en la siguiente tabla, para proteger y conseguir la continuidad del servicio de atención veterinaria.

Descripción del control
Documentación de la infraestructura de IT
Entrenamiento en continuidad de negocio
Realización de copias de seguridad
Almacenamiento de backups onsite y offsite
Control de acceso físico
Sustitutos para el personal clave
Protección contra cortes eléctricos

7.5.1.3. Estrategia de recuperación de la función de negocio

La siguiente tabla contiene las acciones de recuperación que la organización debería acometer para la recuperación del proceso de negocio **Atención Veterinaria** en el caso en el que un incidente inesperado hubiese causado la pérdida o hubiese vuelto inaccesible dicho proceso.

Prioridad de recuperación	Activo	Acciones de recuperación	Responsable	Progreso de la recuperación (tiempo y estatus)
1	Empleados	La persona responsable de la organización y su responsable secundario pueden realizar las acciones que recaen sobre los empleados.	Responsable de la organización	
2	Edificio principal	Una vez se ha contenido la emergencia, volver a implementar las medidas de seguridad física. Hay que asegurar que la batería externa y el SAI funcionan correctamente.	Responsable de la organización	
3	Material veterinario	Determinar si es necesario realizar alguna compra para reemplazar el material dañado.	Responsable Secundario	
4	Red Eléctrica	Hay que asegurar el correcto funcionamiento de la red eléctrica.	Responsable de la organización	
5	Equipamiento veterinario	Hay que asegurar que el equipamiento funciona adecuadamente, a través de la revisión de técnicos especializados.	Responsable Secundario	

6	Winvet	Iniciar el proceso de recuperación para cargar el último backup realizado.	Responsable de la organización	
7	PC principal	Si no es posible emplear el PC Principal, instalar la aplicación Winvet en cualquier otro equipo y cargar el último backup. Contactar con el equipo de soporte de Winvet para asegurar que pueden realizar las tareas de soporte desde el mismo equipo (este paso no es bloqueante para la operación).	Responsable de la organización	

La última columna de la tabla “**Progreso de la recuperación (tiempo y estatus)**” sirve para documentar el estado de la acción de recuperación (tiempo invertido para lograr la recuperación) en caso de incidente y, posteriormente, realizar un análisis de lecciones aprendidas y ajustar su estrategia si el tiempo necesario ha sido superior al RTO.

7.5.2. Proceso de Negocio “Gestión de registros veterinarios”

El proceso de **Gestión de registros veterinarios** es un proceso crítico para la clínica XYZ. La falta de disponibilidad de este proceso puede constituir un problema para la continuidad de operaciones de la clínica, ya que el proceso de Atención Veterinaria requiere a su vez de este proceso. Sin unos registros adecuados, no será posible obtener información del historial clínico de un animal, con el consecuente riesgo que supone para los mismos, y tampoco se dispondrá de un histórico con las actuaciones realizadas sobre

los animales, por lo que existe la posibilidad de que los tratamientos se vea interrumpidos o que incluso no sea posible determinar cuándo una actuación es necesaria.

La **Gestión de registros veterinarios** se realiza mediante el aplicativo Winvet, estando la base de datos de dicho aplicativo en el equipo PC principal.

En caso de un incidente que afecte a este proceso, el equipo podría realizar nuevas actuaciones, siendo necesario que documenten las mismas en papel para que, una vez se recupere el servicio, pueda incluirse esta información en Winvet. Sin embargo, para poder consultar el histórico de actuaciones realizadas sobre un animal, la única alternativa pasa por recuperar el aplicativo, sea en el mismo PC o en uno diferente.

De cara a la contención del incidente o emergencia y a la recuperación de los activos, la compañía dispone de un listado con el contacto de los proveedores con los que se tendrá que coordinar para asegurar la recuperación del proceso. Se almacenará una copia del listado en las instalaciones de la organización y otra copia fuera de las instalaciones.

En cuanto al proceso de negocio y la resiliencia de la clínica, se han definido los siguientes valores:

- MTD: 2 días.
- RPO: 1 día.
- RTO: 4 horas.

7.5.2.1. Formulario de análisis de daños

Se incluye a continuación el formulario que tendrá que ser completado por el responsable del proceso de negocio **Gestión de registros veterinarios** en el momento en el que ocurra un incidente. Así, para cada uno de los activos listados en el formulario, el responsable del proceso tendrá que indicar la gravedad del daño que ha sufrido el activo y cuál es la acción que se sugiere realizar para recuperar el activo (salvar, reparar, recuperar o reemplazar).

Nombre del proceso Gestión de registros veterinarios	Responsable del proceso	Responsable
Activos que soportan el proceso	Daño incurrido (incluyendo evaluador y fecha)	Acción sugerida (Salvar, reparar, recuperar, reemplazar/comprar)
Winvet		
PC principal		
Red Eléctrica		
Empleados		

7.5.2.2. Protección de la función de negocio

La clínica XYZ dispone de ciertos controles de continuidad, descritos en la siguiente tabla, para proteger y conseguir la continuidad del servicio de atención veterinaria.

Descripción del control
Documentación de la infraestructura de IT
Entrenamiento en continuidad de negocio
Realización de copias de seguridad
Almacenamiento de backups onsite y offsite
Protección contra cortes eléctricos

7.5.2.3. Estrategia de recuperación de la función de negocio

La siguiente tabla contiene las acciones de recuperación que la organización debería acometer para la recuperación del proceso de negocio **Gestión de registros veterinarios** en el caso en el que un incidente inesperado hubiese causado la pérdida o hubiese vuelto inaccesible dicho proceso.

Prioridad de recuperación	Activo	Acciones de recuperación	Responsable	Progreso de la recuperación (tiempo y estatus)
1	Empleados	La persona responsable de la organización y su responsable secundario pueden realizar las acciones que recaen sobre los empleados	Responsable de la organización	
2	Winvet	Iniciar el proceso de recuperación para cargar la organización el último backup realizado.	Responsable de la organización	
3	PC principal	Si no es posible emplear el PC Principal, instalar la aplicación Winvet en cualquier otro equipo y cargar el último backup. Contactar con el equipo de soporte de Winvet para asegurar que pueden realizar las tareas de soporte desde el mismo equipo (este paso no es bloqueante para la operación).	Responsable de la organización	
4	Red eléctrica	Hay que asegurar el correcto funcionamiento de la red eléctrica.	Responsable de la organización	

La última columna de la tabla “**Progreso de la recuperación (tiempo y estatus)**” sirve para documentar el estado de la acción de recuperación (tiempo invertido para lograr la recuperación) en caso de incidente y, posteriormente, realizar un análisis de lecciones aprendidas y ajustar su estrategia si el tiempo necesario ha sido superior al RTO.

7.5.3. Proceso de Negocio “Comunicación con clientes”

El proceso de **Comunicación con clientes** es un proceso relevante para la clínica XYZ. La clínica centra su negocio alrededor de la atención individual y personalizada, para conseguir fidelizar a los clientes. Una pérdida del proceso de comunicación con clientes puede suponer la pérdida de estos.

En el proceso de **Comunicación con clientes** los activos involucrados son los empleados, el teléfono, la red telefónica, la red eléctrica y la página web.

De cara a la contención del incidente o emergencia y a la recuperación de los activos, la clínica dispone de un listado con el contacto de los proveedores con los que se tendrá que coordinar para asegurar la recuperación del proceso. Se almacenará una copia del listado en las instalaciones de la organización y otra copia fuera de las instalaciones.

En cuanto al proceso de negocio y la resiliencia de la clínica, se han definido los siguientes valores:

- MTD: 2 horas
- RPO: N/A
- RTO: 30 minutos

7.5.3.1. Formulario de análisis de daños

Se incluye a continuación el formulario que tendrá que ser completado por el responsable del proceso de negocio **Comunicación con clientes** en el momento en el que ocurra un incidente. Así, para cada uno de los activos listados en el formulario, el responsable del proceso tendrá que indicar la gravedad del daño que ha sufrido el activo y cuál es la acción que se sugiere realizar para recuperar el activo (salvar, reparar, recuperar o reemplazar).

Nombre del proceso Comunicación con clientes	Responsable del proceso	Responsable
Activos que soportan el proceso	Daño incurrido (incluyendo evaluador y fecha)	Acción sugerida (Salvar, reparar, recuperar, reemplazar/comprar)
Empleados		
Página Web		
Teléfono		
Red telefónica		
Red eléctrica		

7.5.3.2. Protección de la función de negocio

La clínica XYZ dispone de ciertos controles de continuidad, descritos en la siguiente tabla, para proteger y conseguir la continuidad del servicio de atención veterinaria.

Descripción del control
Documentación de la infraestructura de IT
Entrenamiento en continuidad de negocio
Establecimiento de SLAs para la prestación del servicio de gestión y mantenimiento de la página web
Desvío de llamadas al teléfono de la propietaria

7.5.3.3. Estrategia de recuperación de la función de negocio

La siguiente tabla contiene las acciones de recuperación que la organización debería acometer para la recuperación del proceso de negocio **Comunicación con clientes** en el caso en el que un incidente inesperado hubiese causado la pérdida o hubiese vuelto inaccesible dicho proceso.

Prioridad de recuperación	Activo	Acciones de recuperación	Responsable	Progreso de la recuperación (tiempo y estatus)
1	Empleados	La persona responsable de la organización y su responsable secundario pueden realizar las acciones que recaen sobre los empleados	Responsable de la organización	
2	Red eléctrica	Hay que asegurar el correcto funcionamiento de la red eléctrica.	Responsable de la organización	

3	Red telefónica	Comprobar que es posible realizar llamadas	Responsable Secundario	
4	Teléfono	Comprobar que es posible realizar llamadas	Responsable Secundario	
5	Página web	Revisar que la página web está operativa y con los contenidos adecuados	Responsable Secundario	

La última columna de la tabla “**Progreso de la recuperación (tiempo y estatus)**” sirve para documentar el estado de la acción de recuperación (tiempo invertido para lograr la recuperación) en caso de incidente y, posteriormente, realizar un análisis de lecciones aprendidas y ajustar su estrategia si el tiempo necesario ha sido superior al RTO.

7.5.4. Proceso de Negocio “Gestión de inventarios”

El proceso de **Gestión de inventarios** es un proceso relevante para la clínica XYZ. Si ocurre un incidente con este proceso o el proceso no disponible, es posible que la clínica no disponga de material veterinario para realizar sus actuaciones veterinarias.

En el proceso de **Gestión de inventarios** los activos involucrados son el material veterinario, PC principal, Internet y Router.

De cara a la contención del incidente o emergencia y a la recuperación de los activos, la compañía dispone de un listado con el contacto de los proveedores con los que se tendrá que coordinar para asegurar la recuperación del proceso. Se almacenará una copia del listado en las instalaciones de la organización y otra copia fuera de las instalaciones.

En cuanto al proceso de negocio y la resiliencia de la clínica, se han definido los siguientes valores:

- MTD: 1 día
- RPO: N/A
- RTO: 4 horas

7.5.4.1. Formulario de análisis de daños

Se incluye a continuación el formulario que tendrá que ser completado por el responsable del proceso de negocio **Gestión de inventarios** en el momento en el que ocurra un incidente. Así, para cada uno de los activos listados en el formulario, el responsable del proceso tendrá que indicar la gravedad del daño que ha sufrido el activo y cuál es la acción que se sugiere realizar para recuperar el activo (salvar, reparar, recuperar o reemplazar).

Nombre del proceso Gestión de inventarios	Responsable del proceso	Responsable
Activos que soportan el proceso	Daño incurrido (incluyendo evaluador y fecha)	Acción sugerida (Salvar, reparar, recuperar, reemplazar/comprar)
Material veterinario		
PC principal		
Router		
Red eléctrica		
Internet		
Empleados		

7.5.4.2. Protección de la función de negocio

La clínica XYZ dispone de ciertos controles de continuidad, descritos en la siguiente tabla, para proteger y conseguir la continuidad del servicio de atención veterinaria.

Descripción del control
Documentación de la infraestructura de IT
Entrenamiento en continuidad de negocio
Redundancia de proveedores de material veterinario
Existencia de redes alternativas (red móvil, red doméstica en el domicilio de la propietaria) para realizar pedidos

7.5.4.3. Estrategia de recuperación de la función de negocio

La siguiente tabla contiene las acciones de recuperación que la organización debería acometer para la recuperación del proceso de negocio Gestión de Inventarios, el en caso en el que un incidente inesperado hubiese causado la pérdida o hubiese vuelto inaccesible dicho proceso.

Prioridad de recuperación	Activo	Acciones de recuperación	Responsable	Progreso de la recuperación (tiempo y estatus)
1	Empleados	La persona responsable de la organización y su responsable secundario pueden realizar las acciones que recaen sobre los empleados	Responsable de la organización	
2	Material Veterinario	La persona responsable de la organización revisará el inventario para asegurar que se dispone del mínimo imprescindible y que este se encuentra en buenas condiciones	Responsable de la organización	
3	Edificio	Una vez se ha contenido la emergencia, volver a implementar las medidas de seguridad física. Hay que asegurar que la batería externa y el SAI funcionan correctamente.	Responsable de la organización	
4	Red eléctrica	Hay que asegurar el correcto		

		funcionamiento de la red eléctrica.		
5	Router	Comprobar que se puede navegar. Si se detecta alguna incidencia, contactar con el ISP.	Responsable secundario	
6	Internet	Comprobar que se puede navegar. Si se detecta alguna incidencia, contactar con el ISP.	Responsable secundario	
7	PC Principal	Se asegurará que el PC funciona correctamente. En el caso en el que se detecte algún problema, se reemplazará con alguno de los otros equipos	Responsable secundario	

La última columna de la tabla “**Progreso de la recuperación (tiempo y estatus)**” sirve para documentar el estado de la acción de recuperación (tiempo invertido para lograr la recuperación) en caso de incidente y, posteriormente, realizar un análisis de lecciones aprendidas y ajustar su estrategia si el tiempo necesario ha sido superior al RTO.

7.6. Análisis del riesgo de los activos

A través de la información de los procesos de negocio críticos de la clínica, se ha realizado una primera aproximación al riesgo que presenta cada activo de cara a la continuidad de negocio de la compañía. A raíz de esto se han identificado los activos más críticos de la clínica, los cuales serán el objeto del análisis del riesgo:

- Empleados
- Edificio
- Material veterinario

- Equipamiento veterinario
- Winvet
- PC principal
- Red Eléctrica
- Página Web
- Teléfono
- Red telefónica
- Router
- Internet

Para la estimación del riesgo de estos activos se analizará el impacto que tendría para las funciones críticas de negocio que un determinado activo no esté disponible y la probabilidad de que ese activo no esté disponible.

Para la estimación del impacto se parte del punto anterior y se establecerá un valor al impacto que se calcula como la suma de las prioridades de los procesos críticos en los que el activo tiene una participación, asignando los siguientes valores:

- 3 a las funciones con **prioridad de recuperación alta**,
- 2 a las funciones con **prioridad de recuperación media**,
- 1 a las funciones con **prioridad de recuperación baja**.

ID	Activo	Número de procesos críticos en los que participa	Impacto
1	Empleados	4	10
2	Edificio	2	5
3	Material veterinario	2	5
4	Equipamiento veterinario	1	3
5	Winvet	2	6
6	PC principal	3	8
7	Red Eléctrica	4	10
8	Página Web	1	2
9	Teléfono	1	2
10	Red telefónica	1	2
11	Router	1	2
12	Internet	1	2

Organizaremos el impacto en las siguientes categorías:

- Un valor de 1 o 2, supone un **impacto menor**
- Un valor de 3 o 4 supone un **impacto grave**
- Un valor de 5 o 6 supone un **impacto crítico**
- Un valor de 7 o 8 supone un **impacto mayor**
- Un valor de 9 o 10 supone un **impacto crítico**

Para otorgar un valor a la probabilidad de que alguno de los activos no esté disponible, se ha considerado la información histórica de la compañía, así como nuestro juicio provisional. Se asignará a la probabilidad un valor del 1 al 5, siendo:

- 1 una **probabilidad muy remota** (menos de una vez cada 10 años),
- 2 una **probabilidad remota** (1 vez cada 10 años),
- 3 una **probabilidad baja** (una vez cada 2 años),
- 4 una **probabilidad alta** (1 vez al año)
- 5 una **probabilidad muy alta** (varias veces al año).

Finalmente, se calcula el riesgo de cada activo como el valor de Probabilidad * Impacto. Así, el análisis de riesgos queda como:

ID	Activo	Impacto	Probabilidad	Riesgo
1	Empleados	10	1	10
7	Red Eléctrica	10	5	50
6	PC principal	8	3	24
5	Winvet	6	3	18
2	Edificio	5	1	5
3	Material veterinario	5	2	10
4	Equipamiento veterinario	3	2	6
8	Página Web	2	3	6
9	Teléfono	2	2	4
10	Red telefónica	2	1	2
11	Router	2	2	4
12	Internet	2	3	6

A continuación (*Figura 15*), se pueden visualizar los resultados gráficamente a través de un mapa de calor:

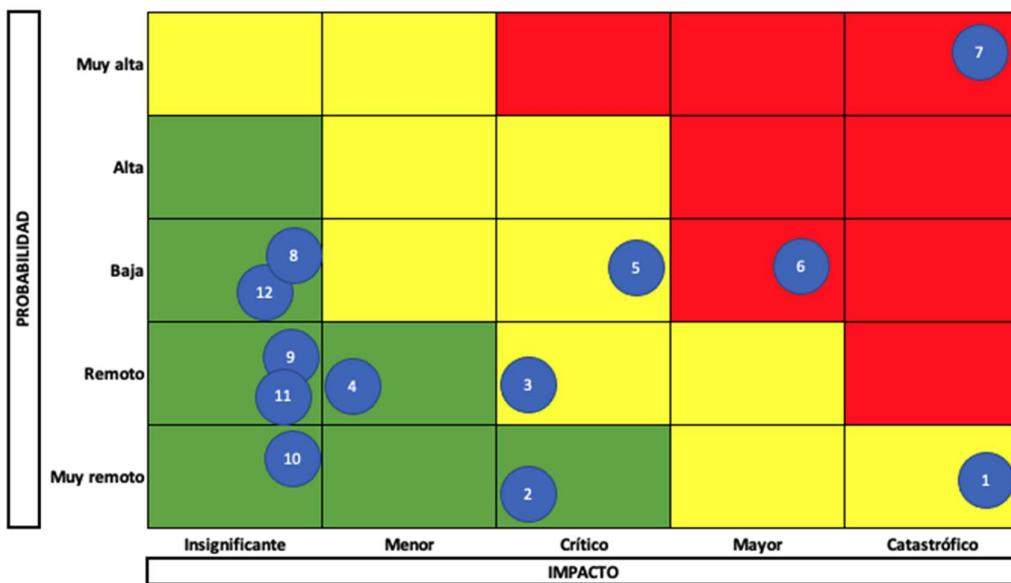


Figura 15: Mapa de calor sin salvaguardas

Tras validar los resultados del análisis anterior con la responsable de la organización, se ha considerado el impacto de los controles compensatorios que ha implementado la entidad. En concreto:

- Para el caso de falta de disponibilidad de la red eléctrica, la entidad ha implementado controles compensatorios para poder dar continuidad a los activos críticos. En concreto, la entidad dispone de un SAI para que el quirófano cuente con energía eléctrica y de una batería externa para poder continuar usando el PC principal. Si bien estas soluciones permiten disponer de electricidad únicamente mientras el SAI y la batería puedan continuar suministrándola, consideramos que la probabilidad de que la red eléctrica no esté disponible durante un tiempo mayor a la capacidad de estos dispositivos es muy remota.
- Para mitigar las consecuencias de la falta de disponibilidad del PC principal, identificamos que la entidad dispone de otros dos PCs (PC secundario 1 y PC secundario 2) que podrían tomar el papel del PC principal. En última instancia, y en el caso extremo en el que ninguno de los 3 PCs esté disponible, la entidad

podría comprar un nuevo PC y empezar a trabajar con él en un tiempo relativamente rápido.

En este punto se ha detectado que la pérdida de datos al levantar Winvet en otro PC podría sobrepasar el RPO indicado por la responsable de la clínica al ser la frecuencia de copias de seguridad guardadas offsite únicamente semanal.

Por tanto, aunque el impacto sobre el proceso de Gestión de Inventarios quedaría mitigado, se sigue considerando que el riesgo no queda mitigado para los procesos de Gestión de Registros Veterinarios y Atención Veterinaria.

- Para el caso de Winvet, acotando la falta de disponibilidad a este aplicativo y no al PC principal, se identifica que la clínica podría emplear las copias de seguridad diarias para restaurar la aplicación. En este caso, al tratarse de copias de seguridad diarias, la pérdida de datos es menor al RPO establecido por la entidad, por lo que el riesgo quedaría mitigado.

Considerando el efecto de estos controles sobre la probabilidad e impacto de los activos involucrados en los procesos de negocio críticos, obtenemos el siguiente resultado:

ID	Activo	Impacto	Probabilidad	Riesgo
6	PC principal	6	3	18
7	Red Eléctrica	10	1	10
1	Empleados	10	1	10
3	Material veterinario	5	2	10
5	Winvet	6	1	6
4	Equipamiento veterinario	3	2	6
8	Página Web	2	3	6
12	Internet	2	3	6
2	Edificio	5	1	5
9	Teléfono	2	2	4
11	Router	2	2	4
10	Red telefónica	2	1	2

Se representa también esta situación a través de un mapa de calor (*Figura 16*).

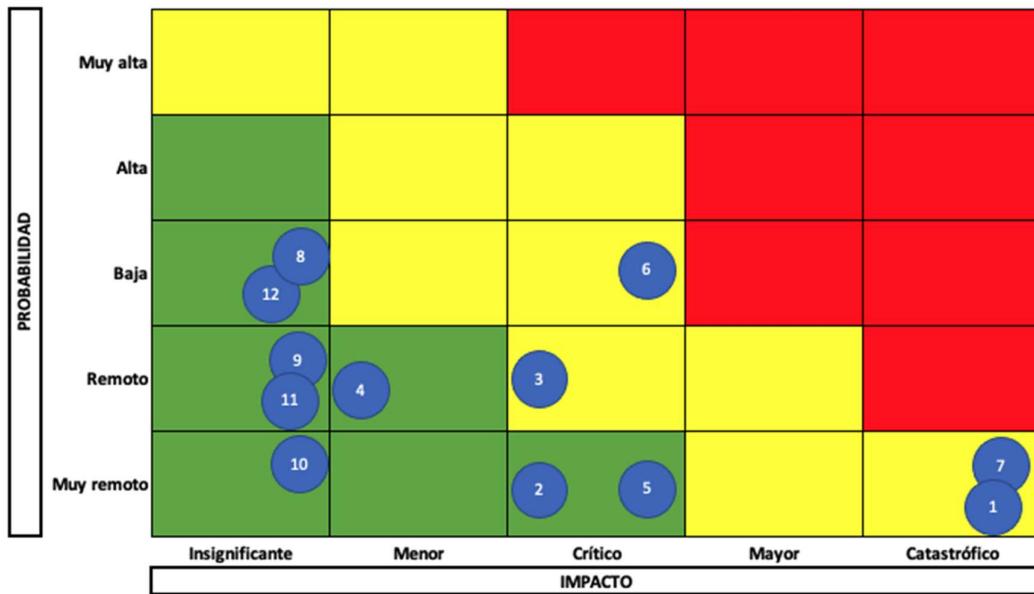


Figura 16: Mapa de calor con salvaguardas

En base a estos resultados, se considera como prioritario establecer un control para mitigar el riesgo de falta de disponibilidad del PC principal. En concreto, y tal y como se ha descrito en el PDS, se considera que es necesario implementar un control para realizar copias de seguridad de Winvet que estén almacenadas fuera del PC principal con una frecuencia de al menos el RPO, de manera que la pérdida de datos no supere el RPO.

El resto de los puntos han sido analizados con la responsable de la clínica, indicando ésta que se encuentra conforme con el nivel de riesgo residual, aceptando los mismos.

7.7. Gestión de Cambios

La persona responsable de XYZ de los cambios posteriores a la finalización del presente documento es el **Propietario del Documento**. Las propuestas de mejora del procedimiento de gestión de acceso se dirigen al propietario del documento, quien una vez al año (o antes si es necesario) evaluará todas las propuestas presentadas y realizará los cambios si aplica, realizando una formación el equipo de continuidad de negocio para que sean conocedores de los cambios.

7.8. Formación del PCN

La formación se debe realizar al menos una vez al año o en el caso de que sea el personal nuevo, el que deba tener responsabilidades en este plan, recibirá también formación una vez sea contratado. El personal de XYZ será formado hasta el punto en que puedan ejecutar sus respectivas responsabilidades de continuidad del negocio sin la ayuda de los documentos. La formación abarca los siguientes aspectos:

- Propósito del PCN.
- Coordinación y comunicación del equipo de continuidad del negocio.
- Procedimientos de informes
- Arreglos de seguridad.
- Procesos específicos del equipo.
- Responsabilidades individuales.
- Simulacros y pruebas del PCN.

7.9. Prueba del PCN

Probar la capacidad para recuperar las funciones críticas del negocio es un componente esencial de una gestión efectiva de la continuidad del negocio. Estas pruebas se deberían realizar periódicamente por parte de XYZ con el alcance y la frecuencia determinados por la criticidad de las funciones de negocio, el papel de XYZ en las operaciones de mercado y los cambios significativos en el negocio de la organización o en su entorno externo. Además, realizando pruebas se identifica la necesidad de modificar el PCN de la clínica XYZ y otros aspectos de la gestión de la continuidad del negocio en respuesta a los cambios en su negocio, responsabilidades, sistemas, software, hardware, personal, instalaciones o entorno externo. Los siguientes elementos deberían ser incorporados a la hora de planificar un ejercicio:

- **Objetivo.** La parte/función de continuidad del negocio del PCN que se va a poner a prueba.
- **Objetivos.** Los resultados previstos. Los objetivos deben ser desafiantes, específicos, medibles, alcanzables, realistas y oportunos.

- **Alcance.** Identifica los departamentos u organizaciones involucradas, la función empresarial crítica, el área geográfica y las condiciones y presentación de la prueba.
- **Aspectos y suposiciones artificiales.** Define qué aspectos del ejercicio son artificiales o supuestos, como información de fondo, procedimientos a seguir y disponibilidad de equipos.
- **Instrucciones para los participantes.** Explica que el ejercicio brinda la oportunidad de probar el PCN antes de un desastre real.
- **Narrativa del ejercicio.** Proporciona a los participantes la información de fondo necesaria, establece el entorno y prepara a los participantes para la acción. Es importante incluir factores como el tiempo, la ubicación, el método de descubrimiento y la secuencia de eventos, si los eventos han concluido o aún están en curso, informes de daños iniciales y cualquier condición externa.
- **Prueba y evaluación posterior al ejercicio.** El ejercicio se supervisa de manera imparcial para determinar si se lograron los objetivos. Se evalúa el desempeño de los participantes, incluyendo la actitud, la decisión, el mando, la coordinación, la comunicación y el control. La sesión informativa posterior es breve pero completa, y explica qué funcionó y qué no, haciendo hincapié en los éxitos y las oportunidades de mejora. La retroalimentación de los participantes también debe incorporarse en la evaluación del ejercicio.

La persona encargada de la continuidad del negocio de la clínica XYZ será el responsable de registrar los ejercicios de preparación del PCN de XYZ en la siguiente tabla:

Fecha	Tipo de ejercicio	Comentarios

7.10. Revisión del PCN

La revisión del plan y de los componentes del plan se debería llevar a cabo anualmente.

Además, se tiene que reevaluar el PCN de la clínica XYZ cuando se produce alguno de los siguientes eventos:

- Cambios regulatorios.
- Cambios en los recursos o en las estructuras organizativas.
- Cambios en el nivel de financiamiento o presupuesto.
- Cuando se producen cambios en el entorno de amenazas o se produce un incidente real o contingencia.
- Cuando se realizan cambios sustanciales en la infraestructura de TI de la organización.
- Después de un ejercicio o simulacro para incorporar los hallazgos.

8. Conclusiones

El presente PDS ha sido elaborado con el objetivo de establecer una estrategia integral para la protección de los activos y la mitigación de los riesgos identificados en la clínica veterinaria XYZ. Durante el proceso de elaboración, se han llevado a cabo análisis exhaustivos, evaluaciones de riesgos y se ha establecido el cronograma para la correcta implementación de los controles de seguridad.

Adicionalmente, se ha realizado un entendimiento de las funciones críticas de negocio de la entidad para establecer el BIA de la entidad y subsecuentemente desarrollar el PCN de la clínica.

8.1. Resumen de los principales hallazgos del TFM

En base al trabajo realizado, consideramos conseguidos los objetivos propuestos al inicio del trabajo:

1. Entendimiento de la organización y su negocio.
2. Creación del inventario de activos de la organización.
3. Desarrollo de un análisis de riesgos de los activos de la entidad, empleando la herramienta PILAR. Identificación de amenazas y evaluación de la probabilidad y el impacto que tienen sobre los activos.
4. Mapeo del marco de control de la organización contra la norma ISO 27002:2013 y selección de controles a implementar.
5. Desarrollo de un PDS para la implementación de los controles identificados en el punto anterior, incluyendo la priorización de las acciones que componen este y la propuesta de un cronograma.
6. Creación de la Política de Seguridad de la Información.
7. Entendimiento de las funciones críticas de negocio, identificando el MTD, RTO y RPO para cada una de ellas.
8. Desarrollo del PCN de la organización, identificando roles y responsables y detallando los controles implementados para asegurar la continuidad de los servicios y las acciones a acometer para lograr la recuperación.

8.2. Limitaciones del estudio

Como limitaciones del presente trabajo hay que indicar que el alcance del mismo se ha descrito en el punto anterior.

También hay que comentar que ha quedado fuera del alcance de este trabajo:

- la implementación de ambos planes de acción (PDS y PCN) propuestos queda fuera del alcance del trabajo.
- la realización de un nuevo análisis de seguridad con el fin de evaluar la adecuación y suficiencia de los controles implementados en el PDS.

8.3. Recomendaciones para futuros trabajos

Como recomendaciones para futuros trabajos, se identifican:

1. Es necesario establecer una función de riesgos dentro de la organización que se encargue de reevaluar de forma periódica los riesgos a los que está expuesta la organización y los controles que la entidad ha implementado para mitigarlos, con objeto de identificar si ha habido algún cambio y es necesario aumentar el nivel de control interno de la organización.
2. Ante los cambios regulatorios que se avecinan, con la puesta en marcha en septiembre de la ya aprobada ley de bienestar animal en marzo de 2023, es necesario realizar un análisis para identificar si existen nuevos requerimientos legales que requieren un cambio en los controles establecidos por la entidad.
3. Dado que la clínica dispondrá ya de un PDS y un PCN, puede ser muy recomendable que siga fortaleciendo su seguridad de la información a través de la implementación formal de un SGSI a través de la ISO 27002, y quizás, ir preparándose para una certificación de dicho SGSI frente a la ISO 27001. Lo mismo con el PNC, que puede ser el punto de partida para una futura certificación en la ISO 22301 de continuidad de negocio.

9. Acrónimos

TFM: Trabajo Fin de Máster.

ISO: International Organization for Standardization.

NIST: National Institute of Standards and Technology.

INCIBE: Instituto Nacional de Ciberseguridad.

PDS: Plan Director de Seguridad.

SMP: Security Master Plan.

BIA: Business Impact Analysis.

PCN: Plan de Continuidad de Negocio.

BCP: Business Continuity Plan.

MTD: Maximum Tolerable Downtime.

RPO: Recovery Point Objective.

RTO: Recovery Time Objective.

SLA: Service Level Agreement.

ISP: Internet Service Provider.

SGSI: Sistema de Gestión de Seguridad de la Información.

10. Índice de Figuras

Figura 1: Modelo de Deming o PDCA	19
Figura 2: Proceso del PDS (Fuente INCIBE)	22
Figura 3: Pasos elaboración PDS	29
Figura 4: Diagrama de red de XYZ	31
Figura 5: Inventario de Activos.....	42
Figura 6: Diagrama de Dependencias.....	44
Figura 7: Probabilidad de las amenazas de las dimensiones de los activos.....	50
Figura 8: Impacto acumulado.....	52
Figura 9: Riesgo acumulado	53
Figura 10: Impacto repercutido.....	54
Figura 11: Riesgo repercutido	55
Figura 12: Cronograma.....	73
Figura 13: Evolución impacto acumulado	76
Figura 14: Evolución riesgo acumulado	76
Figura 15: Mapa de calor sin salvaguardas	98
Figura 16: Mapa de calor con salvaguardas.....	100

11. Referencias bibliográficas

11.1. Lista de las fuentes consultadas para la elaboración del TFM

1. ISO 27001 Técnicas de seguridad para tecnologías de la información:
<https://www.iso.org/standard/54534.html>
2. NIST Framework de Ciberseguridad:
<https://www.nist.gov/cyberframework>
3. ISO 22301 Gestión de la continuidad de negocio:
<https://www.iso.org/standard/75106.html>
4. INCIBE PDS:
<https://www.INCIBE.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad>

11.2. Bibliografía

1. World Economic Forum, «Global Cybersecurity Outlook 2023 INSIGHT REPORT,» Enero 2023. [En línea]. Available:
https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf.
2. INCIBE, «Balance de ciberseguridad 2022,» [En línea]. Available:
https://www.INCIBE.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2022_INCIBE.pdf.
3. Australian Cyber Security Centre. [En línea]. Available:
https://www.cyber.gov.au/sites/default/files/2023-03/ACSC_Small_Business_Guide_A4_First_Nations_0.pdf.
4. Report: Animal care companies need to heed cybersecurity calls too. The Daily Record. [En línea]. Available:
<https://thedailyrecord.com/2022/09/20/report-animal-care-companies-need-to-heed-cybersecurity-calls-too/>.

5. Un hacker atemoriza a los veterinarios madrileños: roba datos personales de los clientes. Vozpopuli. [En línea]. Available:
<https://www.vozpopuli.com/espana/veterinarios-hacker-clientes.html>.
6. «UNE-EN ISO/IEC 27000:2021 [Recurso electrónico]: Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario. (ISO/IEC 27000:2018),» 2021.
7. [En línea]. Available: www.iso27000.es.
8. M. d. H. y. A. Públicas, «MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método,» [En línea]. Available:
<https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>.
9. INCIBE, «PDS. Colección Protege tu Empresa,» [En línea]. Available:
https://www.INCIBE.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf.
10. INCIBE. «PLAN DE CONTINGENCIA Y CONTINUIDAD DE NEGOCIO. Colección Protege tu Empresa,» [En línea]. Available:
https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf.
11. Banco de España. [En línea]. Available:
https://www.bde.es/f/webbde/COM/Supervision/politica/ficheros/es/Recomendaciones_relativas_a_la_continuidad_del_negocio.pdf.
12. INCIBE. [En línea]. Available:
https://www.INCIBE.es/sites/default/files/contenidos/dosieres/plan-director-seguridad/plan_director_de_seguridad_hoja_de_verificacion_controles.xls.

12. Anexos

12.1. Política de la Seguridad de la información

En XYZ nos comprometemos a proteger la confidencialidad, integridad y disponibilidad de la información de nuestros pacientes, propietarios de mascotas y el funcionamiento general de la clínica. Esta política establece las directrices y responsabilidades para garantizar la seguridad de la información.

1. Alcance

Esta política se aplica a todos los empleados, contratistas, proveedores y terceros que interactúen con la información de la clínica veterinaria, ya sea en formato físico o digital.

2. Responsabilidades

a. Dirección de la Clínica Veterinaria

- Proporcionar recursos adecuados para implementar y mantener las medidas de seguridad de la información.

b. Empleados

- Cumplir con esta política y las medidas de seguridad de la información establecidas.
- Reportar cualquier incidente de seguridad o sospecha de violación a la Dirección.

3. Clasificación de la Información

a. Categorías de Información

- Se establecerán controles y niveles de acceso basados en la clasificación de la información.

b. Tratamiento de la Información Confidencial

- La información confidencial debe ser protegida de divulgación no autorizada y utilizada solo para fines legítimos.

4. Seguridad Física

- Las áreas de la clínica veterinaria donde se almacena información sensible deben ser aseguradas con cerraduras y acceso restringido.
- Los documentos físicos deben ser almacenados en armarios o archivadores seguros cuando no se estén utilizando.

5. Seguridad de la Tecnología de la Información

a. Acceso a los Sistemas

- Se implementarán controles de acceso basados en roles y privilegios para garantizar que solo el personal autorizado pueda acceder a los sistemas y datos correspondientes.
- Se fomentará el uso de contraseñas seguras y su cambio periódico.

6. Uso Apropriado de los Recursos

- Los recursos informáticos y de red de la clínica veterinaria se utilizarán exclusivamente para fines laborales.
- El uso inapropiado, como la descarga o el acceso a contenido no relacionado con el trabajo, está estrictamente prohibido.

7. Concienciación y Capacitación

- Se fomentará la cultura de seguridad mediante la educación sobre la importancia de la seguridad de la información.

8. Revisiones y Actualizaciones

- Esta política se revisará periódicamente para asegurar su relevancia y efectividad.
- Los cambios significativos en los riesgos o requerimientos legales relacionados con la seguridad de la información serán considerados para actualizar esta política.

Al implementar esta política de seguridad de la información, XYZ estará mejor preparada para proteger los datos confidenciales de sus pacientes y garantizar la continuidad de sus operaciones.

