Trabajo fin de Máster

Grado en ingeniería de tecnologías de telecomunicación

Universidad de Valladolid

Gestión de Riesgos en Ciberseguridad

Autor:
Inés Varona Peña

Tutor:
Rubén Mateo Lorenzo Toledo

Septiembre 2023

Agradecimientos

En primer lugar, quiero agradecer a mi tutor, Rubén, por su orientación, paciencia y dedicación a lo largo de todo el proceso. Gracias por los consejos y la disposición a resolver todas mis dudas y preguntas.

Agradezco especialmente a mis compañeros de carrera y amigos, quienes me han brindado su apoyo y motivación en todo momento, y han compartido conmigo sus conocimientos y experiencias.

Por último, quiero expresar mi gratitud a mi familia, en especial a mis padres quienes han sido mi principal fuente de apoyo y motivación en mi formación académica y personal.

Sin la ayuda y colaboración de todas estas personas, este trabajo no habría sido posible.

Gracias a todos vosotros.

Resumen

La seguridad de la información se ha vuelto crucial para las organizaciones en un mundo cada vez más interconectado y digitalizado. La gestión de riesgos en seguridad de la información desempeña un papel fundamental al identificar, evaluar, mitigar y supervisar amenazas para proteger los activos críticos y garantizar la continuidad operativa en un entorno complejo.
Dentro de este ámbito, la gestión de activos de ciberseguridad se destaca al proporcionar una visión completa y actualizada de los recursos de tecnología de la información. Esta gestión es vital, ya que cualquier dispositivo, recurso o servicio en una infraestructura puede ser vulnerable, lo que podría desencadenar ataques más amplios.
La metodología EBIOS, respaldada por la ANSSI y recomendada por la ENISA, ofrece un enfoque estructurado y detallado para identificar activos y evaluar riesgos, convirtiéndose en una de las mejores opciones disponibles. La categorización de activos según esta metodología facilita la organización y clasificación de elementos críticos, fortaleciendo así la estrategia de gestión de riesgos.

Para obtener un inventario centralizado, es imprescindible unificar y cruzar datos de diversas fuentes con el objetivo de deshacerse de los datos dispersos en diferentes formatos y bases de datos, lo que dificulta la gestión de activos y riesgos. A través de un esfuerzo de recopilación, normalización y consolidación de datos, se puede lograr crear un inventario centralizado de activos de tecnología de la información.
Una vez obtenido este inventario centralizado, a través de la herramienta Power BI se puede crear un dashboard que transforma los datos en una representación visual y altamente comprensible. Esta herramienta simplifica la gestión de riesgos al proporcionar una forma visual de comparar el nivel de impacto por aplicación con la importancia de cada una para la empresa.

Índice

1. Introducción

En los últimos años, la importancia de la seguridad de la información se ha incrementado significativamente en las empresas, esto se debe a la creciente interconexión de sistemas y comunicaciones que se basan en el intercambio de datos. El avance de la digitalización y la adopción de nuevas tecnologías han expuesto la información a riesgos en un entorno previamente desconocido. A medida que la digitalización simplifica la gestión de la información, también se incrementa la cantidad de amenazas y vulnerabilidades a las que esta se encuentra expuesta.

Un incidente de seguridad tiene el potencial de impactar varios activos de información, lo que a su vez podría poner en peligro las operaciones de una empresa y, en última instancia, su estabilidad. La información que gestiona una empresa es de vital importancia y, como tal, debe recibir un tratamiento adecuado y cuidadoso debido a su relevancia. Desde una perspectiva económica, la pérdida de información crítica puede dar lugar a problemas significativos.

La gestión de riesgos constituye un procedimiento esencial en el contexto de la seguridad de la información y la ciberseguridad. Este proceso involucra la identificación, evaluación, mitigación y supervisión de los riesgos que pueden influir en una organización. Su propósito primordial es salvaguardar los activos críticos de la organización, que pueden comprender datos, sistemas, redes e infraestructuras, asegurando al mismo tiempo la continuidad de sus operaciones en un entorno caracterizado por su creciente complejidad y amenazas constantes.

Este trabajo se enfoca en una de las etapas clave de la gestión de riesgos: la identificación y valoración de riesgos. En este contexto, la identificación se refiere a la identificación precisa de todos los activos de la organización, entendiendo que estos activos pueden abarcar desde servidores y aplicaciones hasta datos sensibles y otros recursos relevantes. Por otro lado, la valoración implica comprender la importancia y el valor de cada uno de estos activos en el contexto operativo de la empresa, así como los riesgos que pueden afectarlos.

Actualmente, en la mayoría de las empresas contemporáneas, existe un desafío significativo en la gestión de activos. La información sobre estos activos suele dispersarse en diversas fuentes, como hojas de cálculo, bases de datos y escaneos de red, lo que conduce a un descontrol y falta de visibilidad sobre los activos críticos. Esta falta de cohesión en la gestión de activos puede resultar en una protección deficiente contra amenazas cibernéticas y dificultar la toma de decisiones informadas en materia de seguridad.

El propósito central de este trabajo es proponer un método efectivo para el inventario de activos que resuelva este problema de descontrol y dispersión de información. Este método permitirá reunir toda la información sobre los activos en un único repositorio centralizado, lo que facilitará la identificación y valoración de riesgos de manera más precisa y eficiente. Además, proporcionará una base sólida para la toma de decisiones estratégicas en seguridad cibernética.

Este trabajo se estructura en una serie de secciones esenciales que abarcan diversos aspectos relacionados con la gestión de activos de ciberseguridad y la seguridad de la información. Estos componentes cruciales guían la exploración y el análisis en profundidad de la temática abordada.

La primera sección del trabajo (hitos y planificación) proporciona una visión general de cómo se ha desarrollado el proyecto, destacando los hitos clave que marcaron su evolución. Aquí se detalla la planificación estratégica que se ha seguido para llevar a cabo cada fase del proyecto, permitiendo una comprensión clara de su desarrollo cronológico y sus logros significativos. Se

ha empleado un diagrama de Gantt para visualizar y organizar de manera efectiva el desarrollo del proyecto a lo largo del tiempo.

La siguiente sección, el marco teórico, se adentra en los conceptos fundamentales relacionados con la seguridad de la información y la gestión de riesgos. Se explora en profundidad el alcance y la importancia de la seguridad de la información, y se explica con detalle las distintas fases de la gestión de riesgos, poniendo de relieve cómo se desarrollan y en qué consisten. Esta base teórica sienta las bases necesarias para comprender la relevancia de la gestión de activos en el contexto de la seguridad informática.

El tercer apartado del trabajo presenta la metodología empleada para llevar a cabo la gestión de activos. Se describen los elementos clave considerados en este proceso, resaltando las herramientas y estrategias específicas utilizadas para gestionar de manera eficiente los activos de ciberseguridad. Esta sección proporciona una visión detallada de cómo se ha implementado la gestión de activos en la práctica. Se ha utilizado la herramienta Power BI para crear y desarrollar el panel de control (dashboard) que ha permitido la visualización de datos de manera eficiente y la generación de informes precisos que respaldan la toma de decisiones informadas.

En la sección de resultados, se exponen los hallazgos obtenidos a partir de un caso de uso real. Se analizan los activos afectados por una vulnerabilidad específica actual y se muestra cómo la gestión de activos permite evaluar y abordar esta situación de manera efectiva.

Las proyecciones futuras para el trabajo se esbozarán en la penúltima sección, delineando posibles direcciones para avanzar en la gestión de activos de ciberseguridad y en la mejora continua de la seguridad de la información. Este apartado plantea oportunidades para la expansión y el desarrollo futuro de la investigación.

La sección de conclusiones resume y enfatiza la importancia de la gestión de activos en el ámbito de la seguridad de la información. Se destacan los principales descubrimientos y aprendizajes obtenidos a lo largo del trabajo, proporcionando una visión general del impacto y las implicaciones de la gestión de activos de ciberseguridad en la práctica empresarial y tecnológica.

2. Hitos y planificación

La planificación general del proyecto se ha mantenido en general en línea con el plan inicial. Sin embargo, hubo ciertos ajustes y desafíos inesperados a lo largo del camino. En particular, los primeros días del proyecto requirieron más tiempo del previsto originalmente debido a la necesidad de comprender conceptos nuevos y complejos. Esta etapa inicial de aprendizaje resultó crucial, ya que implicaba la familiarización con estándares y metodologías de gestión de riesgos cibernéticos, lo que llevó un poco más de tiempo de lo anticipado.

Uno de los desafíos significativos en esta fase inicial fue descubrir que, aunque todos los estándares de gestión de riesgos persiguen objetivos similares, cada uno tiene sus propios pasos y terminología específica. Esto hizo que la lectura y comprensión de múltiples estándares fuera una tarea más ardua de lo que se esperaba.

Además, la lectura de los estándares en sí misma resultó ser una tarea laboriosa, ya que estos documentos suelen ser extensos y técnicos. La comprensión profunda de su contenido llevó más tiempo de lo previsto.

En cuanto a la parte práctica del proyecto, la unificación de fuentes de datos y la normalización de los datos demostraron ser procesos más largos de lo anticipado. Cada archivo de Excel y base de datos presentaba diferencias en la estructura y nomenclatura de los datos, lo que requirió esfuerzos adicionales para unificarlos y asegurar que los datos se representaran de manera coherente en el inventario centralizado.

Asimismo, el proceso de cruzar datos de diferentes fuentes y garantizar su integridad y precisión resultó ser una tarea que demandó más tiempo de lo inicialmente estimado. Esto se debió a la complejidad de correlacionar y vincular datos de múltiples fuentes de manera coherente.

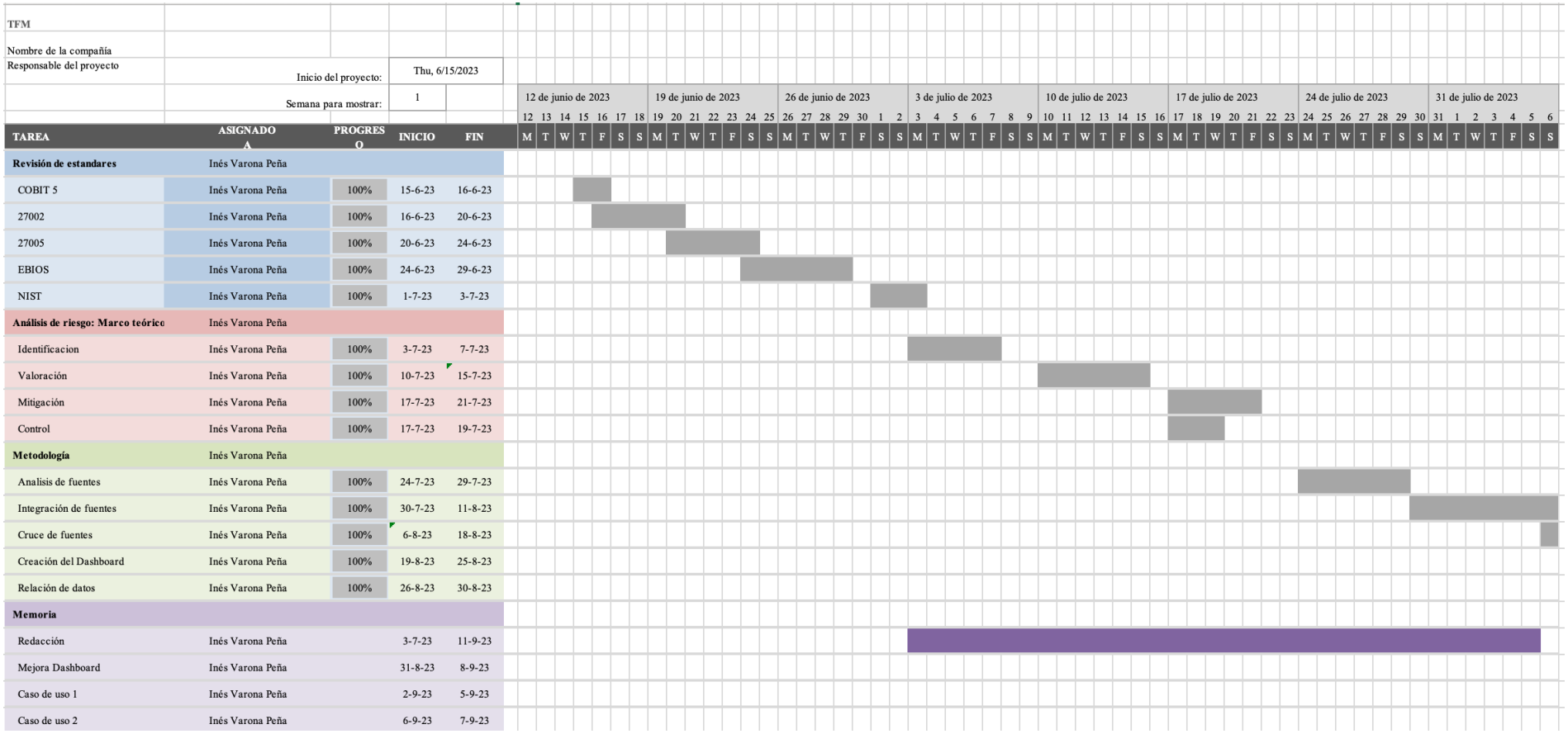


Figura 1: Diagrama de Gantt previsto.

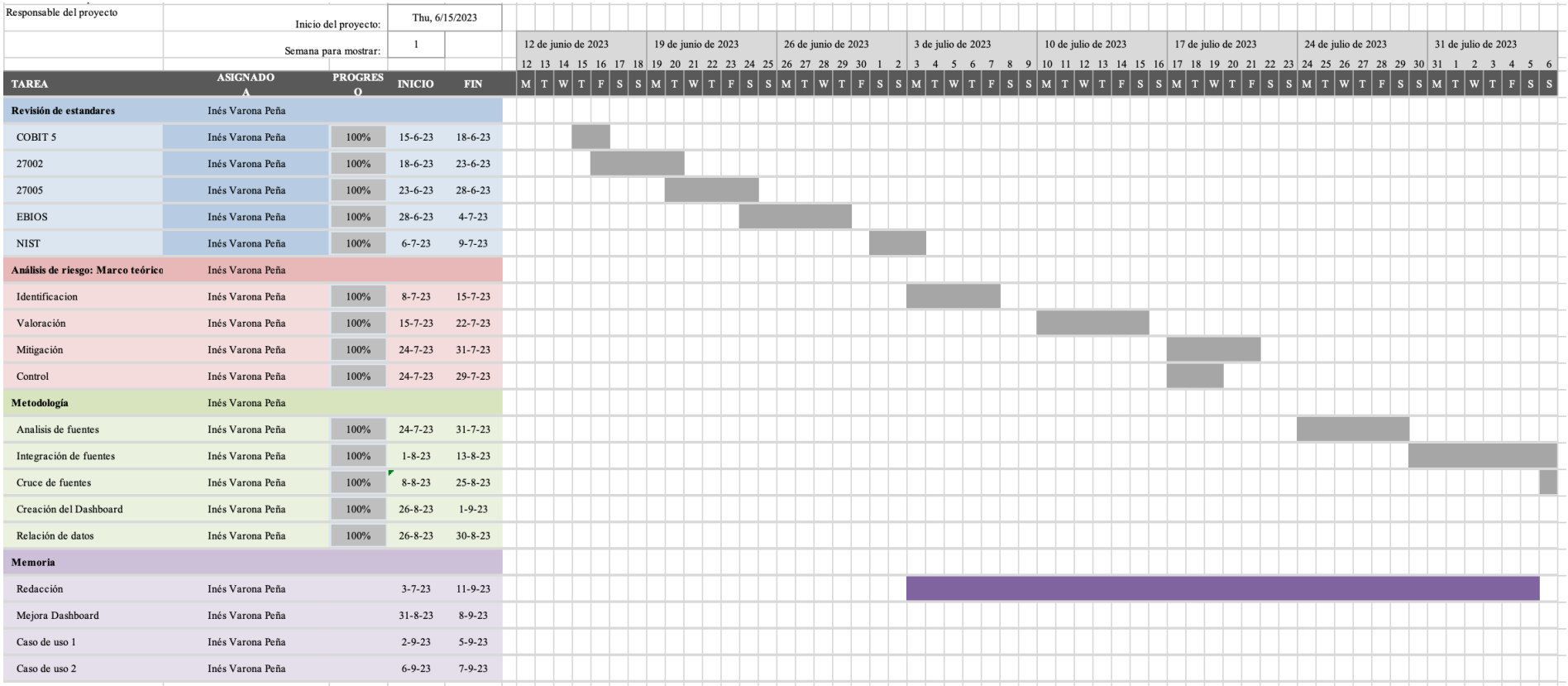


Figura 2: Diagrama de Gantt real.

3. Marco Teórico

Históricamente, la información ha representado un recurso estratégico de gran poder, y, por lo tanto, la seguridad de la información se ha convertido en un elemento esencial para cualquier organización que necesite guardar y proteger sus activos (información a proteger).

Durante siglos, la seguridad de la información se ha aplicado en sistemas de información tradicionales, donde la información se almacenaba en formatos orales o escritos, como papiros, pergaminos o papel. Sin embargo, con la llegada de las tecnologías de la información y las comunicaciones, estos sistemas de información han evolucionado hacia sistemas informatizados, en los que la información se introduce, procesa y almacena en medios electrónicos. En la actualidad, en la era de las comunicaciones digitales, la información se transmite a través de medios telemáticos. Este cambio de paradigma ha dado lugar al surgimiento del campo de la ciberseguridad.

Con el transcurso del tiempo se han definido tres principios o propiedades fundamentales que ha de tener la información, la denominada triada de la información:

1. Confidencialidad: la información solo tiene que ser accesible o divulgada a aquellos que están autorizados.
2. Integridad: la información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros.
3. Disponibilidad: la información debe estar siempre accesible para aquellos que estén autorizados.

[Instituto Nacional de Ciberseguridad, 2016]

Figura 3: Triada de la información. Adaptado de [Instituto Nacional de Ciberseguridad, 2016].

3.1. Seguridad de la información, seguridad informática y ciberseguridad

Cuando se menciona el término **ciberseguridad**, es necesario considerar varios conceptos simultáneamente. Entre ellos se debe hablar del concepto de seguridad, según la Real Academia Española (RAE), seguro se define como: "libre o exento de todo peligro, daño o riesgo" [RAE,]. Sin embargo, en la actualidad, alcanzar un estado completamente seguro se ha vuelto utópico debido a la evolución de las conexiones y las comunicaciones, que han agregado nuevos riesgos

a los ya existentes.

Si bien es cierto que el término ciberseguridad no está recogido explícitamente en el diccionario de la Real Academia Española (aunque ha sido ampliamente adoptado y utilizado en el ámbito tecnológico y de la seguridad), se puede comprender su definición al analizar la composición de la palabra.
Por un lado, el prefijo "ciber-" se define como "relacionado con redes informáticas". Por otro lado, "seguridad" se define como "la cualidad de estar seguro". De esta manera, al combinar ambos elementos, podemos entender que la ciberseguridad se refiere a las medidas y prácticas relacionadas con la protección de los sistemas informáticos y las redes contra amenazas y riesgos cibernéticos. Se trata, por tanto, de garantizar la integridad, confidencialidad y disponibilidad de la información en el entorno digital, así como proteger los sistemas y las redes contra ataques y vulnerabilidades. Para la Asociación de Auditoría y Control sobre los Sistemas de Información (ISACA), la ciberseguridad es "la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".[ISA, 2021, Martínez, 2018].

Conceptos históricamente relacionados a la ciberseguridad son la seguridad de la información y la seguridad informática. El primer concepto, también conocido como *information security* puede describirse a partir de las definiciones contenidas en la norma ISO 27001. En esta norma se define como información: "aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración". Además, define que la seguridad de la información, "consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización".[International Organization for Standardization, 2013].

La norma ISO/IEC 27002:2021 por otra parte define *computer security* o seguridad informática como: "La preservación de la confidencialidad, integridad y disponibilidad de la información procesada por un sistema informático." [Organización Internacional de Normalización, 2013].

Llegado a este punto se tienen tres conceptos muy parecidos: ciberseguridad, seguridad de la información y seguridad informática. En vista de las definiciones anteriores se tiene que los conceptos son similares, pero no intercalables.

Es importante resaltar que la Seguridad de la Información abarca un alcance más amplio que la Ciberseguridad y la Seguridad Informática, su objetivo principal es proteger la información en todas sus formas y estados frente a posibles riesgos que puedan afectarla.
La seguridad informática engloba un conjunto de procesos, técnicas y herramientas diseñadas para proteger tanto los sistemas informáticos (redes e infraestructura) como la información en formato digital; esto incluye la seguridad de sistemas que no están conectados a la red.
Por otra parte, la Ciberseguridad (abarcada en la seguridad informática) se centra únicamente en los formatos digitales presentes en sistemas interconectados o conectados a una red. [Lisa Institute,]

Figura 4: Esquema seguridad de la información, seguridad informática y ciberseguridad.

A medida que se profundiza en la comprensión de los términos clave como ciberseguridad, seguridad informática y seguridad de la información, que se han visto anteriormente; se revela su impacto directo en el establecimiento de un entorno protegido. Sin embargo, la mera conceptualización no es suficiente; la implementación efectiva de estos principios requiere una estrategia holística. Es aquí donde el ciclo de vida de la arquitectura de seguridad entra en juego, trascendiendo la teoría y proporcionando un marco práctico para la planificación, análisis, acción y monitoreo continuo de medidas de seguridad integrales.

3.2. Ciclo de vida de la seguridad de la información

En las últimas décadas, se ha presenciado una notable transformación en los requisitos de seguridad de la información manejada por las organizaciones. En sus comienzos, la seguridad de la información se basaba en enfoques físicos y procedimientos administrativos. Sin embargo, con la aparición y el constante progreso de los sistemas informáticos, ha emergido una necesidad apremiante: la creación de soluciones automáticas para resguardar archivos y otros datos almacenados en memoria. Estas demandas de seguridad han propiciado la evolución de los sistemas operativos, orientándolos hacia la protección de los recursos del sistema y la restricción del acceso únicamente a usuarios debidamente autorizados.[Mengual Galán, 2005].

Esta evolución se alinea con el concepto del ciclo de vida de la arquitectura de seguridad, que abarca la planificación, implementación, monitoreo y adaptación constante de las estrategias de seguridad en un entorno en constante cambio. En un mundo interconectado, donde el desarrollo simultáneo de sistemas distribuidos y redes de datos ha introducido desafíos de seguridad asociados a la distribución de información, el ciclo de vida de la arquitectura de seguridad desempeña un papel crucial. Este ciclo asegura la continua adaptación de las medidas de seguridad a los nuevos riesgos. La incorporación de funcionalidades de seguridad en las arquitecturas de comunicación, como parte de este ciclo, garantiza una protección eficiente y adaptable en un entorno tecnológico en constante evolución.[Mengual Galán, 2005].

El ciclo de vida de la arquitectura de seguridad, basado en el enfoque de la ISACA [1] (Systems Audit and Control Association), se compone de cuatro etapas clave: planificar, analizar, actuar y

[1]Organización profesional global que se dedica a la promoción y el desarrollo de prácticas de auditoría, control y seguridad de sistemas de información.

monitorear. Estas etapas se interconectan para formar un proceso continuo y cíclico que asegura la eficacia y la adaptabilidad de la arquitectura de seguridad en un entorno tecnológico en constante evolución.[ISACA, 2018a].

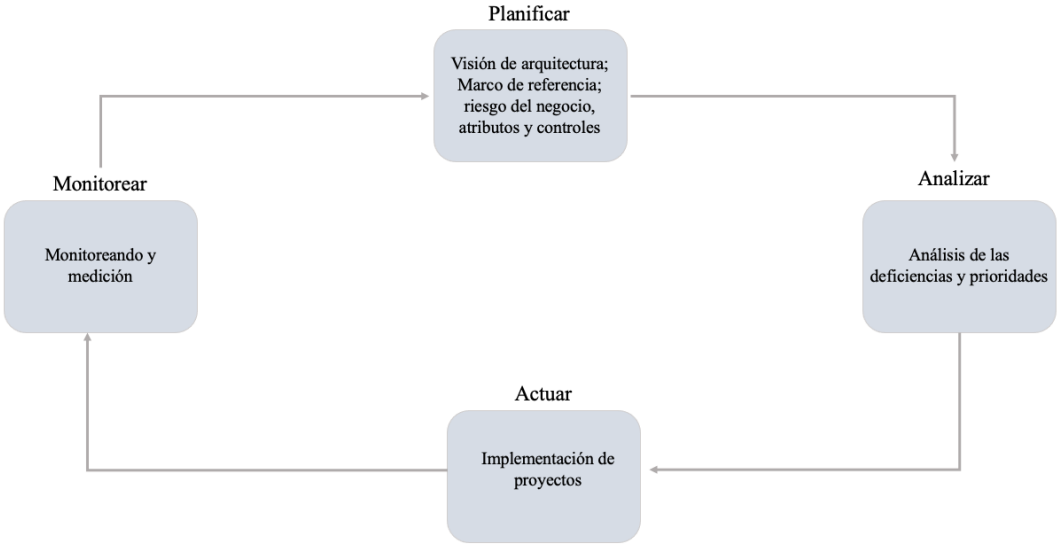


Figura 5: Ciclo de vida de la arquitectura de seguridad.[ISACA, 2018a].

- Planificar: en la etapa de planificación, se delinean los objetivos de seguridad, estrategias y requisitos específicos para la arquitectura de seguridad. Esto involucra la identificación de activos críticos, la evaluación de amenazas y riesgos potenciales, y el establecimiento de controles de seguridad. También se definen los indicadores para medir el éxito de las medidas implementadas.
- Analizar: una vez establecidos los objetivos y requisitos, se ingresa a la fase de análisis. Aquí, se realiza un análisis exhaustivo de las soluciones de seguridad disponibles y se evalúa su adecuación a las necesidades organizativas. Se consideran aspectos como la viabilidad técnica, la eficacia y el costo de implementación. También se identifican posibles vulnerabilidades y áreas que demandan atención adicional.
- Actuar: con la planificación y el análisis realizados, se procede a la etapa de acción. Aquí es donde se ejecutan las medidas de seguridad definidas en las etapas anteriores. Esto podría involucrar la instalación y configuración de sistemas de seguridad, la formulación de políticas y procedimientos, la capacitación del personal y otras acciones destinadas a robustecer la arquitectura de seguridad.
- Monitorear: la fase de monitoreo es esencial en el ciclo de vida de la arquitectura de seguridad. Implica la supervisión constante de las medidas implementadas para asegurar su funcionamiento adecuado y su adaptación a las cambiantes amenazas y requisitos. Se establecen sistemas de monitoreo y alerta para detectar y responder a incidentes de seguridad en tiempo real. Además, se realiza evaluaciones periódicas para identificar oportunidades de mejora y optimización en la arquitectura de seguridad.

Estas cuatro etapas se integran en un ciclo continuo en el cual la planificación, el análisis, la acción y el monitoreo convergen para establecer una arquitectura de seguridad sólida y adaptable

a las necesidades y desafíos siempre cambiantes de la organización. Una vez establecido el ciclo de vida de la arquitectura de seguridad, es fundamental considerar cómo se establece y mantiene un control efectivo en todo el entorno tecnológico. En este sentido, el gobierno de seguridad emerge como un elemento esencial para garantizar la coherencia y el cumplimiento de las políticas y procedimientos implementados.[ISACA, 2018a]

3.3. Gobierno de seguridad de la información

Para que la seguridad de la información aborde de manera efectiva los constantes desafíos de proporcionar una protección adecuada para los activos de información, es fundamental una estrategia de seguridad de la información. Esta estrategia documenta la dirección y las metas para el programa de seguridad de la información, según lo determine la alta dirección. Posteriormente, la estrategia establece la base para implementar un gobierno efectivo de seguridad de la información. El gobierno, también llamado *governance* o gobernanza, se define (de manera general) como la reglas que dirigen la organización que incluyen políticas, estándares y procedimientos que se utilizan para establecer la dirección y controlar las actividades de la organización. [isa, 2021].

Según el centro criptológico nacional (CCN), la governanza es una capa organizativa que contemple aquellos aspectos complementarios a la tecnología necesarios para asegurar que la ciberseguridad y la seguridad de la información se entiendan como un proceso ordenado y metodológico dirigido a garantizar la ciberresiliencia de los procesos de negocio.
Implica la implementación de políticas, procedimientos y procesos para gestionar y supervisar adecuadamente las actividades de seguridad informática, seguridad de la información y ciberseguridad en una organización. Es un marco de referencia que busca asegurar que las estrategias de seguridad estén alineadas con los objetivos y metas de la organización, y que los recursos se utilicen de manera eficiente para proteger la información y los activos de la organización. [Centro Criptológico Nacional, 2022].

La información se puede definir como "datos dotados de significado y propósito". Desempeña un papel fundamental en todos los aspectos de nuestras vidas. Los datos e información almacenados en los sistemas de tecnologías de la información son valiosos y cruciales para el negocio de la organización, ya que el valor de una empresa se concentra en el valor de su información. En un creciente número de compañías, la información es el negocio. [Gashgari et al., 2017, isa, 2021].
Aproximadamente el 80 % de las infraestructuras críticas nacionales en el mundo desarrollado están bajo el control del sector privado. Sin embargo, la protección de estos recursos de información vitales para nuestra supervivencia recae principalmente en el ámbito corporativo debido a la presencia de burocracias ineficientes con numerosas jurisdicciones conflictivas y la decadencia de algunas instituciones que no pueden adaptarse adecuadamente al aumento de los delitos informáticos en el mundo.[isa, 2021, Gashgari et al., 2017].
A pesar de esta responsabilidad, los estudios continúan demostrando que un gran porcentaje de organizaciones no abordan adecuadamente tanto los problemas de seguridad emergentes como los ya existentes. Los resultados de la Encuesta Global de Seguridad de la Información 2015 realizada por *Ernst and Young* resaltan este preocupante problema. Según la encuesta:

- Sólo el 12 % de las organizaciones creen que la seguridad de la información satisface las necesidades de la organización, y el 67 % todavía está haciendo mejoras.
- El 69 % observó que el presupuesto de seguridad de la información debe aumentar hasta

un 50 %, para que pueda proteger a la organización en línea, con la tolerancia al riesgo establecidos por la gerencia.

El informe concluye que las deficiencias en la seguridad de la información son principalmente el resultado de fallas en el ámbito del gobierno y no pueden ser resueltas únicamente mediante soluciones tecnológicas. La Seguridad de la Información aborda la seguridad de los activos de información de manera integral, involucrando a todas las partes interesadas en la organización. Por lo tanto, la seguridad de la información no debe considerarse solo como un problema técnico del departamento de tecnologías de la información, sino como un desafío de gobernanza.
La protección efectiva de los recursos de información requiere un enfoque desde el nivel directivo, al igual que otras funciones críticas de gobierno, para tener éxito. Es decir, abordar adecuadamente la seguridad de la información debe ser planteado y asumido como una responsabilidad clave por parte de la alta dirección de las organizaciones. Solo así se podrá asegurar una protección adecuada contra amenazas emergentes y existentes en el mundo digital. [isa, 2021, Gashgari et al., 2017].

El objetivo del gobierno de la seguridad de la información es desarrollar, implementar y gestionar un programa de seguridad que alcance los siguientes seis resultados básicos:

1. Alineación estratégica:
    - La seguridad de la información se alinea con la estrategia de negocio para respaldar los objetivos de seguridad establecidos por los requerimientos del negocio.
    - Se desarrollan requisitos plenamente desarrollados que proporcionan una orientación clara sobre las acciones a tomar y cuándo se han alcanzado los objetivos.
    - Se ajustan las soluciones de seguridad en los procesos de la empresa, considerando factores como la cultura, el estilo de gobierno, la tecnología y la estructura organizativa.
    - La inversión en seguridad de la información se adapta para ser congruente con la estrategia y las operaciones de la empresa, basándose en un perfil bien definido de amenazas, vulnerabilidades y riesgos.
2. Gestión de riesgos:
    - Se implementan medidas apropiadas para mitigar los riesgos y reducir el posible impacto en los recursos de información a un nivel aceptable, esto incluye comprender colectivamente el perfil de amenazas, vulnerabilidades y riesgos de la organización.
    - Se evalúa la exposición al riesgo y las posibles consecuencias de la inestabilidad: la gestión de riesgos se prioriza teniendo en cuenta las posibles consecuencias, y se llevan a cabo suficientes acciones de mitigación para lograr consecuencias aceptables del riesgo residual. Además, se considera la aceptación o transferencia del riesgo con base en un entendimiento completo de la exposición y las posibles consecuencias.
3. Entrega de valor:
    - Se optimiza la inversión en seguridad de la información para respaldar los objetivos del negocio. Esto incluye mantener un conjunto estándar de prácticas de seguridad y gastos generales en seguridad de la información en un nivel mínimo, pero sin comprometer la efectividad.

- Se establece un programa de seguridad que permite a la organización alcanzar sus objetivos estratégicos.
- Se priorizan y distribuyen los esfuerzos de seguridad en áreas que tienen las mayores probabilidades de impacto y beneficio para el negocio.
- Soluciones institucionales y de uso general basadas en estándares con la mayor relación costo/efectividad.

4. Optimización de recursos:

   - Utilizar el conocimiento de la infraestructura de seguridad de la información de manera eficiente y efectiva, asegurando la captación y disponibilidad de conocimientos relevantes.
   - Documentar los procesos y prácticas de seguridad para establecer una base sólida.
   - Desarrollar una arquitectura de seguridad que defina el uso eficiente de los recursos de la infraestructura.

5. Medición del desempeño:

   - Monitorizar y reportar los procesos de seguridad de la información para garantizar el logro de los objetivos. Esto incluye definir y acordar un conjunto significativo de medidas alineadas con los objetivos estratégicos, proporcionando información valiosa para la toma de decisiones en los niveles estratégicos, gerenciales y operativos.
   - Se establece un proceso de medición que ayuda a identificar deficiencias y proporciona retroalimentación sobre los avances para resolver problemas. Además, se considera el aseguramiento independiente proporcionado por evaluaciones y auditorías externas.
   - Se establecen criterios para distinguir las métricas más relevantes entre la variedad de aspectos que se pueden medir.

6. Integración del proceso de aseguramiento:

   - Se integran todos los factores de aseguramiento pertinentes para garantizar el correcto funcionamiento de los procesos desde el inicio hasta el final. Esto implica determinar todas las funciones de aseguramiento y organizar sus roles.
   - Se desarrollan relaciones formales con otras áreas de aseguramiento y se coordina el trabajo conjunto para lograr una seguridad más rentable.
   - Se asegura que se definan claramente los roles y responsabilidades entre las funciones de asesoramiento, evitando que se superpongan o se omita alguna protección.
   - Se emplea un enfoque de sistemas para la planificación, implementación, medición y gestión de la seguridad de la información, garantizando una gestión cohesiva y efectiva de los recursos.

[isa, 2021].

A medida que exploramos el papel fundamental del gobierno en el contexto de la seguridad de la información, surge un componente crucial que no puede pasarse por alto: la gestión de riesgos (como se acaba observa arriba en el texto). El gobierno establece el marco y las directrices para la toma de decisiones y la implementación de políticas de seguridad, pero es en la gestión de riesgos donde estas directrices se traducen en acciones concretas. La gestión de riesgos, como una extensión natural del gobierno, permite una evaluación sistemática de los riesgos

asociados con las operaciones y activos de la organización. Al abordar riesgos potenciales de manera estructurada y proactiva, el gobierno y la gestión de riesgos trabajan en conjunto para salvaguardar la integridad de la organización y sus activos digitales en un mundo cada vez más interconectado y dinámico.

3.4. Gestión de riesgos

Para asegurar que una organización tenga éxito y se mantenga firme, es vital manejar los riesgos de manera adecuada. Aquí entra en juego algo muy importante: los activos. Estos activos son recursos valiosos que tienen y que necesitan proteger en caso de problemas. Entender bien qué son estos activos y cómo se relacionan con la forma en que se manejan los riesgos es esencial para detectar y reducir cualquier problema que los pueda afectar.

3.4.1. Conceptos

El paso inicial en la gestión de riesgos consiste en aclarar la naturaleza de los activos. Una definición precisa de activos abarca elementos valiosos en una organización, tales como información, aplicaciones, servidores, equipos, bases de datos, personas, edificios e infraestructuras. Alternativamente, se puede considerar que los activos son todo lo que deseamos proteger. De acuerdo con el Instituto Nacional de Ciberseguridad, un activo se refiere a cualquier recurso empresarial necesario para las actividades diarias, cuya ausencia o deterioro conlleva una pérdida o coste.[Instituto Nacional de Ciberseguridad, 2016, García, 2019].

Los activos, como componentes a proteger, son susceptibles a vulnerabilidades. Una vulnerabilidad denota una debilidad o punto frágil en nuestros activos. En presencia de activos, estos pueden exhibir puntos vulnerables que señalan a terceros las deficiencias de la organización, aumentando su potencial para sufrir ataques. Las vulnerabilidades pueden adoptar diversas formas, como problemas en aplicaciones (errores), versiones obsoletas (sistema operativo, firmware), políticas defectuosas o fallos humanos. Según el Instituto Nacional de Ciberseguridad, una vulnerabilidad se refiere a la fragilidad que presentan los activos, facilitando la materialización de amenazas.[García, 2019, Instituto Nacional de Ciberseguridad, 2016, Briceño, 2021].

Las amenazas, que debemos diferenciar de adversidades o ataques, indican la posibilidad de aprovechar una vulnerabilidad. Sin vulnerabilidad, no existen amenazas. Las amenazas pueden ser externas o internas, además, pueden surgir de manera accidental o intencionada. En ambos casos, provienen de una fuente, que por lo general se compone de dos factores: el actor que amenaza y la motivación que lo impulsa. Este autor puede ser una persona, grupo, organización o incluso una entidad gubernamental. La motivación puede variar ampliamente y se relaciona con el grupo de actores o los activos que están en riesgo. Puede estar relacionada con publicidad, ganancias financieras, causas políticas o religiosas.[García, 2019, Briceño, 2021]

La materialización de una amenaza sobre un activo, aprovechando su vulnerabilidad, conlleva un impacto o consecuencia para la organización. La noción de vulnerabilidad suele emplearse de forma binaria: algo .es vulnerable.o "no es vulnerable". No obstante, en la mayoría de los casos, los activos poseen diferentes grados de vulnerabilidad. Esto significa que ciertas condiciones de control pueden representar una alta vulnerabilidad, mientras que otras indican una vulnerabilidad menor. El impacto se estima generalmente en una escala del 0 al 10, donde el 10 denota la

pérdida total del activo. [Instituto Nacional de Ciberseguridad, 2016, isa, 2021, Briceño, 2021].

La siguiente figura (6) muestra las relaciones entre los conceptos previamente explicados:

Figura 6: Activo, amenaza, vulnerabilidad e impacto.[Instituto Nacional de Ciberseguridad, 2016].

Cuando las vulnerabilidades que existen en el entorno, quedan expuestas a su amenazas, pueden conseguir tener un impacto sobre nuestros activos, entonces aparecen los riesgos. La tradicional evaluación de riesgos se expresa en la ecuación amenazas + vulnerabilidades + activos = riesgo. El resultado es que, si hay más amenazas frente a más o mayores vulnerabilidades, hay más riesgo. [isa, 2021]

Figura 7: Componentes del riesgo: activos, amenaza, vulnerabilidad. Adaptado de [García, 2019].

Otra definición actual y más generalizada del riesgo, surge en la norma ISO 73:2009, es "la combinación de la probabilidad de un evento y sus consecuencias". Cada vez más, el concepto de consecuencia, está incluido en la ecuación de riesgo, que resulta en amenazas + vulnerabilidades + consecuencias = riesgo.[isa, 2021]

Esto es consistente con la definición actual de riesgo que es la probabilidad de un evento y sus consecuencias. La probabilidad en este caso se deriva de la probabilidad de que una amenaza explota una vulnerabilidad. La relevancia está en el hecho de que si no hay consecuencias como el riesgo no es importante y puede ser considerado inexistente .

La probabilidad, es una medida de la frecuencia en que puede ocurrir un evento. Por tanto, se refiere a la posibilidad de que una amenaza específica aproveche una vulnerabilidad expuesta.

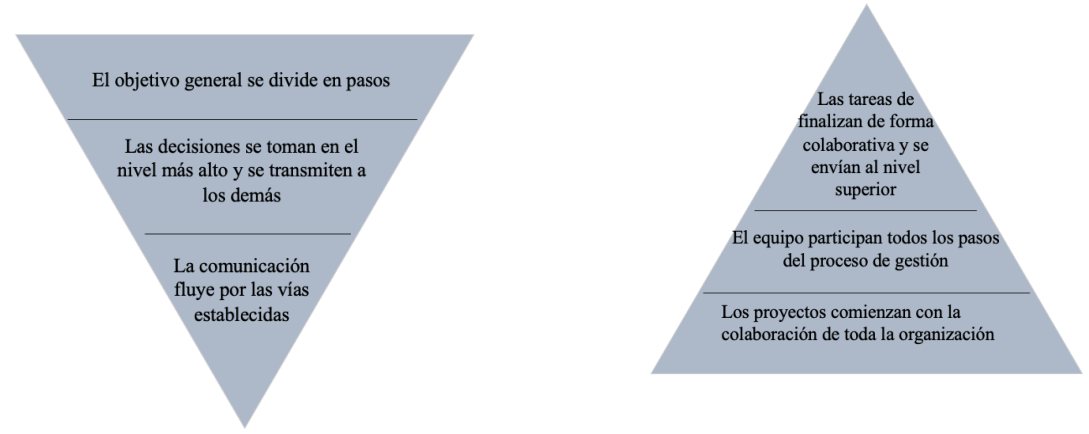
Cuando se identifica el riesgo, la probabilidad se utiliza para calcular el nivel de riesgo en base a la cantidad de eventos combinado con el impacto que pudiera ocurrir en un determinado periodo de tiempo, generalmente un año.Cuanto mayor es la frecuencia, mayor probabilidad y, en consecuencia, mayor el riesgo. [isa, 2021, García, 2019, Instituto Nacional de Ciberseguridad, 2016].

Figura 8: Cálculo del riesgo. Adaptado de [Instituto Nacional de Ciberseguridad, 2016].

3.4.2. Enfoque

A medida que las amenazas cibernéticas se vuelven más sofisticadas y persistentes, las organizaciones se enfrentan al desafío de establecer estrategias efectivas para salvaguardar sus activos digitales. En este contexto emergen dos enfoques principales: el enfoque *top-down* (descendente) y el *bottom-up* (ascendente).

El enfoque de gestión *top-down* representa una de aquellas estrategias en las cuales el proceso de toma de decisiones se ejecuta en los niveles jerárquicos superiores, para posteriormente comunicarse al resto del equipo de trabajo. En el enfoque *bottom-up*, sin embargo, el proceso de toma de decisiones se origina en los niveles inferiores de la jerarquía organizacional y luego se comunica o presenta a los niveles superiores para su consideración. [Asana, 2023].



(a) Enfoque descendente *(top-down)*. (b) Enfoque ascendente (*bottom-up*).

Figura 9: Enfoques.[Asana, 2023].

En el contexto de este trabajo, se ha decidido adoptar un enfoque de gestión *top-down* estricto. A pesar de la tendencia hacia enfoques híbridos, el enfoque descendente tiene su valor en situaciones donde la estructura y la planificación meticulosa son fundamentales. Al abordar el trabajo con esta perspectiva, se espera poder gestionar eficientemente los aspectos complejos del proyecto.
Además, el enfoque top-down, al ser más rígido y estructurado, resulta particularmente adecuado para proyectos que requieren una claridad definida en los objetivos y la dirección desde el

inicio. Al utilizar este enfoque, los responsables de la toma de decisiones establecen una visión global y luego desglosan las acciones necesarias para alcanzarla. Dado que este trabajo implica múltiples componentes y una organización precisa de los procesos, se considera que este enfoque proporcionará la coherencia y la orientación necesarias para lograr los resultados deseados.

3.4.3. Proceso

La gestión de riesgos engloba una serie de procedimientos que consideran los requisitos integrales para la identificación, análisis, evaluación y mantenimiento de niveles de riesgo aceptables. Por lo general, involucra los siguientes procesos:

- Establecimiento del alcance de los límites: el proceso de definición de los parámetros globales para el desempeño de la gestión de riesgos dentro de una organización implica tener en cuenta tanto los factores internos como los externos para proporcionar un contexto adecuado.
- Identificación y valoración de los activos de la información: el proceso de evaluación e inventario de activos consiste en determinar los activos en riesgo y evaluar posibles impactos de una eventual exposición.
- Realización de evaluación del riesgo: proceso consiste en la identificación , el análisis y la evaluación del riesgo, que incluye:
  - La identificación de amenazas, vulnerabilidades y exposiciones, viables.
  - El análisis del nivel de riesgo y el posible impacto.
  - La evaluación de si el riesgo cumple con los criterios de aceptación.
- Determinación del tratamiento de la respuesta al riesgo: el proceso de elección de estrategias para el manejo de los riesgos identificados que superan los niveles aceptables implica la selección de enfoques adecuados. Las estrategias de tratamiento de riesgos incluyen evitar el riesgo mediante la interrupción de actividades de riesgo, mitigar el riesgo a través del desarrollo y la implementación de controles, transferir el riesgo a terceros, ya sea dentro o fuera de la organización, y aceptar el riesgo. Generalmente, se opta por estas estrategias si es factible, si no existe una manera rentable de reducirlo, si la exposición al riesgo es baja, o si no es viable abordarlo de manera efectiva. También involucra la aceptación del riesgo residual, la decisión y aprobación de la alta gerencia para aceptar el riesgo residual ocurre al finalizar el proceso de tratamiento. Esto significa que el riesgo puede ser aceptado una vez que la evaluación demuestre que se encuentra dentro de los límites aceptables o cuando no existe una opción de tratamiento efectiva disponible.
- Comunicación sobre el riesgo y su monitoreo: la comunicación del riesgo suele llevarse a cabo entre los tomadores de decisiones y otras partes involucradas tanto internas como externas a la organización. A través de la comunicación y el monitoreo, se mantienen actualizados y pertinentes el alcance, los límites, la revaluación y los planes de acción.

[isa, 2021].

El flujo de trabajo la respuesta a riesgo se muestra en la figura 10.

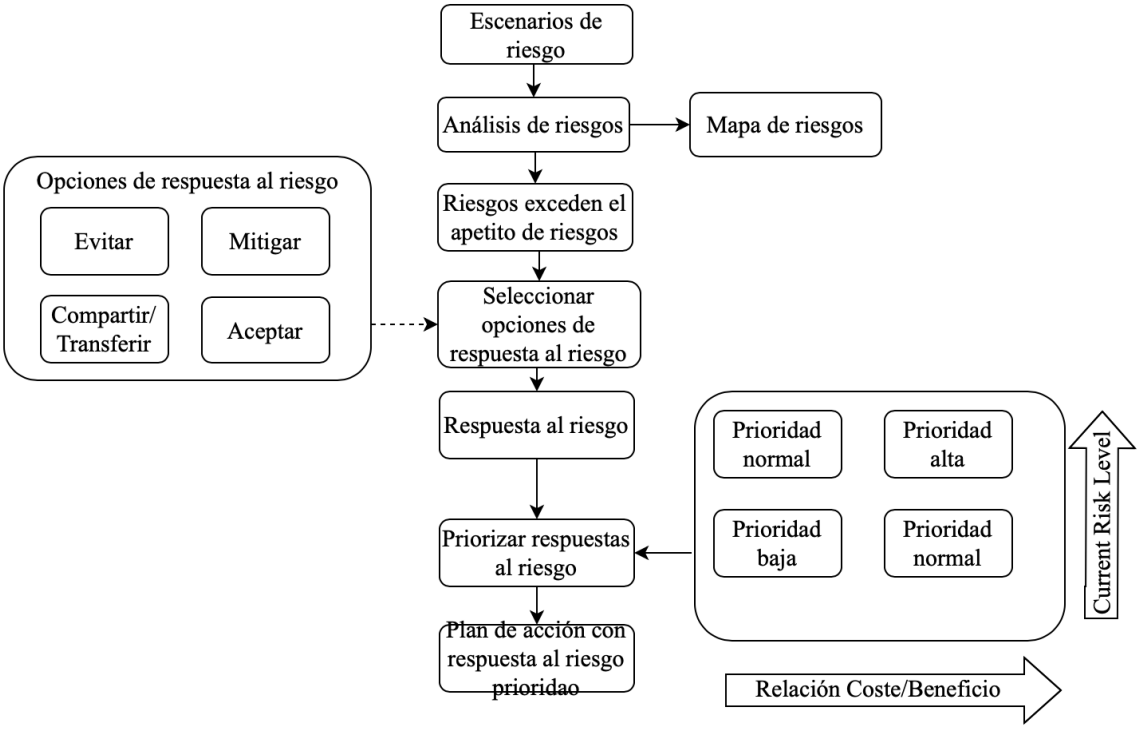


Figura 10: Flujo general de trabajo de respuesta a riesgos. Adaptado de [isa, 2021].

Se observa que, a menudo, se refiere a los conceptos, evitar, reducir, compartir y aceptar utilizando diferentes términos con significado similar:

- Cesar la actividad (evitar).
- Reducir el riesgo (mitigar).
- Transferir el riesgo (compartir).
- Retener el riesgo (aceptar).

Dado que la gestión de riesgos constituye un proceso ininterrumpido, conviene reconocer que dicho proceso sigue un ciclo de vida específico. este ciclo incluye las fases de evaluación, tratamiento y supervisión,como se ejemplifica (de manera simplificada) en la figura 11. Al adoptar un enfoque de gestión de riesgos anclado en este ciclo de vida e integrarlo con la gestión de cambios, es posible optimizar los costos al no requerir una evaluación exhaustiva de riesgos en intervalos regulares. En lugar de ello, es viable realizar ajustes incrementales tanto a la evaluación de riesgos como a los procedimientos de gestión, logrando así una mejora continua. [García, 2019, isa, 2021].

Figura 11: Ciclo simplificado de la gestión continua de riesgos. Adaptado de [isa, 2021].

La gestión de riesgos se caracteriza por ser un proceso constante, iterativo y adaptable, que en todas y cada una de sus fases puede desglosarse en:

- Comunicación y consulta: esta actividad engloba todas las siguientes, ya que se lleva a cabo en todas las etapas. A través de ella se promueve la participación y se coordina la colaboración de todas las partes involucradas, tanto internas como externas, en la gestión de riesgos.

- Establecimiento del contexto: fase inicial y fundamental en el proceso de gestión de riesgos. En esta etapa, se busca obtener una comprensión clara y completa de todos los elementos que influyen en la gestión de riesgos en un entorno específico. Implica definir el alcance del proceso de gestión de riesgos, identificar las partes interesadas relevantes y comprender sus objetivos, necesidades y expectativas.

- Evaluación del riesgo: una vez definido el contexto se han de valorar los riesgos. En esta etapa se determinan los riesgos que van a ser controlados por medio de su identificación, análisis y evaluación. Todos aquellos riesgos que no sean identificados quedarán como riesgos ocultos o no controlados.

- Tratamiento del riesgo: después del proceso de identificación y priorización, se pasa a la fase de actuación, fase en la que se implantan medidas (contramedidas) y controles para reducir (el impacto) de los riesgos. Es necesario poder establecer, para cada una de las actuaciones, su relación coste-beneficio (sin la cual no es posible implantar políticas, ni estrategias, ni evaluar los resultados). En esta fase, debe disponerse de políticas, procedimientos, guías, soluciones tecnológicas claramente redactadas, identificadas y documentadas, soportadas por las estructuras organizativas para su despliegue (tanto en los aspectos administrativos y jurídico-legales como tecnológicos o de gestión).

- Monitorización del riesgo: después de identificar e implantar soluciones, se deben ver los resultados en una monitorización continuada que permita analizar la eficiencia de los con-

troles y contramedidas desplegados. La cuantificación continuada permitirá una mejora continuada de la gestión del riesgos.

[García, 2019, Instituto Nacional de Ciberseguridad, 2016].

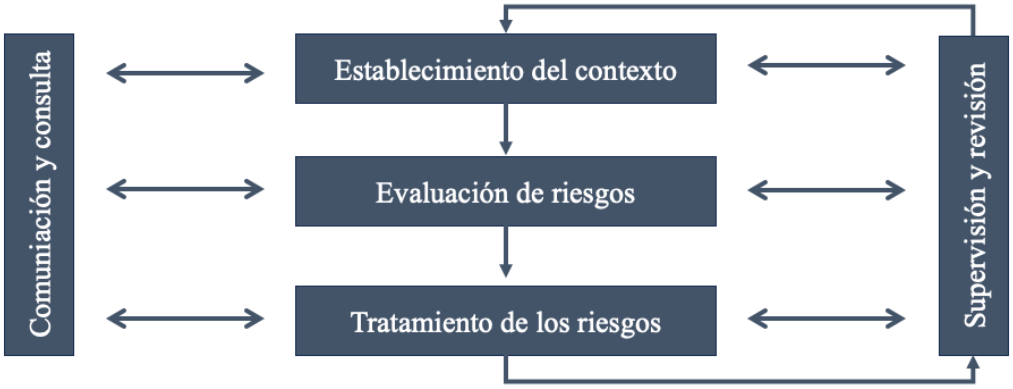


Figura 12: Proceso de la gestión continua de riesgos. Adaptado de [isa, 2021].

3.4.4. Establecimiento de contexto

El contexto involucra el alcance de las actividades de gestión de riesgos y el entorno en el que opera la gestión de riesgos, incluyendo la estructura organizacional y la cultura.
[Instituto Nacional de Ciberseguridad, 2016, isa, 2021].

Es esencial llevar a cabo la identificación de controles preexistentes para evitar redundancias y costos superfluos, como la duplicación de esfuerzos en la implementación. Además, mientras se identifican estos controles, es recomendable llevar a cabo una revisión para garantizar su correcto funcionamiento. Los controles que se tienen previsto implementar como parte de los planes de tratamiento de riesgo deben ser abordados de la misma manera que aquellos que ya están en funcionamiento. Si un control existente que se planea implementar se considera ineficaz, insuficiente o injustificado, es importante revisarlo cuidadosamente para determinar si es necesario eliminarlo o reemplazarlo con una alternativa más adecuada.

La determinación del contexto de la gestión de riesgos implica definir el alcance de la organización y los procesos o actividades a evaluar. Esto abarca el alcance completo de las actividades de gestión de riesgos, así como la identificación de los roles y responsabilidades de las diferentes partes de la organización involucradas en el proceso de gestión de riesgos. También se considera la cultura de la organización en términos de su disposición o aversión a los riesgos. También implica definir los criterios básicos, por ejemplo, se ha de decidir si se va a utilizar un enfoque global o un enfoque detallado; el primero sea más rápido pero menos preciso que el segundo.[Instituto Nacional de Ciberseguridad, 2016, isa, 2021].

Es esencial que la gestión de riesgos se integre tanto con las demás áreas de la empresa como con su entorno externo. Como resultado, es necesario identificar tanto los factores internos como los externos que definen el marco de trabajo. A nivel interno, se consideran aspectos como la

cultura, los recursos, los procesos y los objetivos del negocio. A nivel externo, se analizan diversos aspectos relacionados con el entorno social, económico o legislativo.
[Instituto Nacional de Ciberseguridad, 2016, isa, 2021].

De esta etapa surgirán:

- Establecer los objetivos de la gestión de riesgos.
- Definir los criterios que se emplearán para la evaluación de riesgos, el método para determinar probabilidades y las magnitudes de los impactos.
- Especificar el alcance de la gestión de riesgos, los roles y la asignación de responsabilidades.

[Instituto Nacional de Ciberseguridad, 2016, isa, 2021].

Para desarrollar un programa sistemático de gestión de riesgos de una organización, se debe utilizar un modelo de referencia del Marco general de seguridad de la información que adaptarlo a las circunstancias de la organización.

El modelo de referencia reflejará el estado deseado discutido. Hay varias normas/publicacines disponibles para dar orientación sobre los enfoques de gestión de riesgos de seguridad y de tecnologías de la información. [isa, 2021].
Los ejemplos incluyen:

- *COBIT 5 for Risk*
- *National Institute os Standars and Technology (NIST) Special Publication 800-39: Managing Information Security Risk.*
- *National Cybersecurity Agency of France (ANSSI)*: EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)
- *ISO 31000:2009: risk management-principles and guidelines*
- *ISO/IEC 27005:2011: Information technology- Security techniques- Information security risk magagement.*
- OCTAVE (Evaluación de la Amenaza Operacionalmente Crítica, Activos y Vulnerabilidad; Operationally Critical Threat, Asset, and Vulnerability Evaluation) en sus tres versiones, OCTAVE S, Allegro y FORTE.
- MAGERIT (Metodología de Análisis y Gestión de Riesgos de IT).

[isa, 2021].

COBIT 5

Objetivos de Control para las Tecnologías de la Información y Relacionadas (COBIT, en inglés: Control Objectives for Information and related Technology) es una guía de mejores prácticas presentada como *framework* [2], dirigida al control y supervisión de tecnología de la información (TI). Mantenida por ISACA (en inglés: Information Systems Audit and Control

[2]marco de trabajo

Association) y el IT GI [3] (en inglés: IT *Governance Institute*), tiene una serie de recursos que pueden servir de modelo de referencia para la gestión de TI, incluyendo un resumen ejecutivo, un framework, objetivos de control, mapas de auditoría, herramientas para su implementación y principalmente, una guía de técnicas de gestión. Su primera edición fue publicada en 1996 y consta de 5 principios: [isa, 2021].

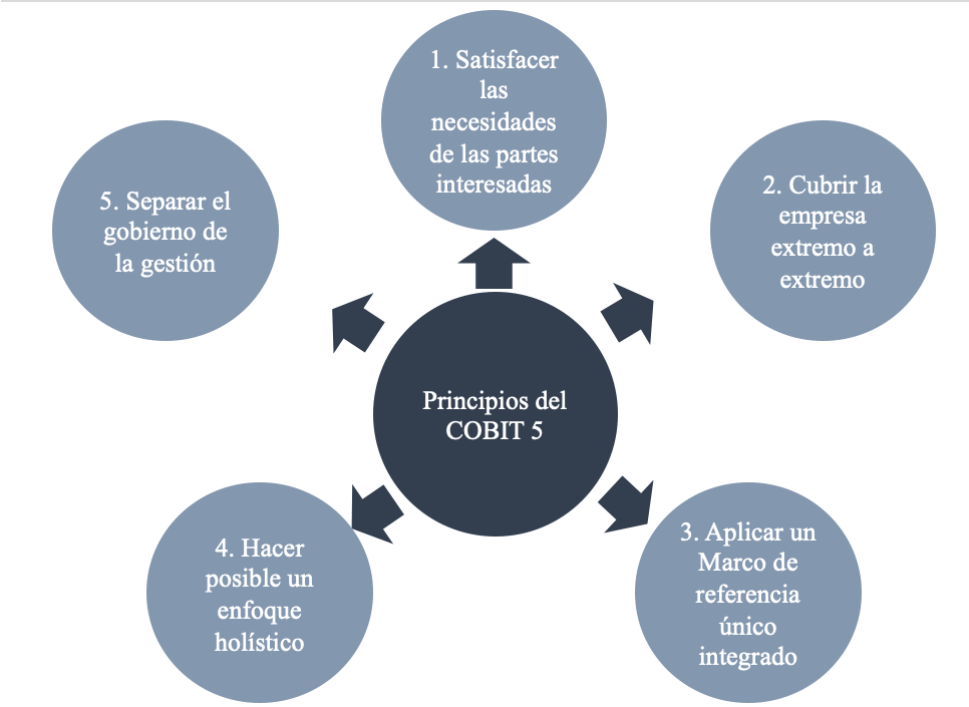


Figura 13: Principios del COBIT 5. Adaptado de [isa, 2021].

NIST

El Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) es una agencia no reguladora que promueve la innovación mediante avances en metrología, normas y tecnología. El Marco de Ciberseguridad del NIST (NIST CSF, NIST Cybersecurity Framework) consta de normas, pautas y mejores prácticas que ayudan a las organizaciones a mejorar su gestión del riesgo de ciberseguridad.

El NIST CSF está diseñado para ser lo suficientemente flexible como para integrarse con los procesos de seguridad existentes de cualquier organización, en cualquier sector. Proporciona un excelente punto de partida para implementar gestión de riesgos de ciberseguridad y seguridad de la información en prácticamente cualquier organización del sector privado en los Estados Unidos. [IBM,].

El Instituto Nacional de Estándares y Tecnología (NIST) del Departamento de Comercio de los Estados Unidos lanzó en 2018 la versión 1.1 de su conocido Marco para Mejorar la Ciberseguridad de Infraestructura Crítica, más ampliamente conocido como el Marco de Ciberseguridad:

[3]Es una asociación profesional independiente para secretarios de empresas, asesores en gobernanza y gestores de riesgos en Australia, comprometida en promover prácticas sólidas en gobernanza y gestión de riesgos.

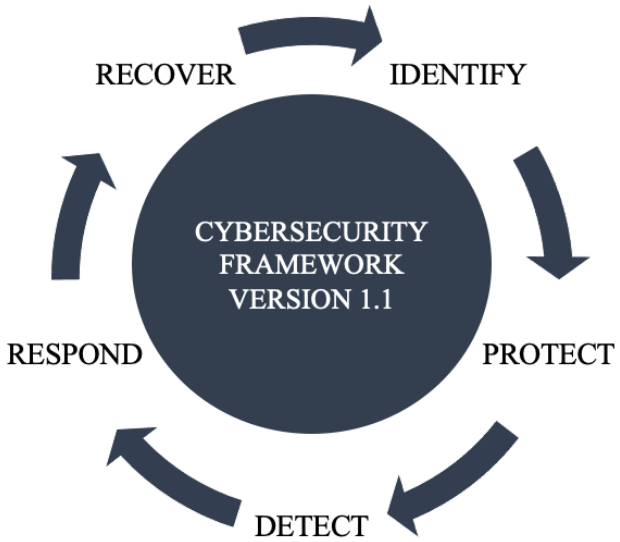


Figura 14: Framework NIST 1.1. Adaptado de [nis,].

ANSII

EBIOS Risk Manager (EBIOS RM) es un método de evaluación y tratamiento de riesgos digitales desarrollado por la Agencia Nacional de Ciberseguridad de Francia (ANSSI) en colaboración con el Club EBIOS. Ofrece una caja de herramientas adaptable cuyo uso varía según los objetivos del proyecto. EBIOS Risk Manager es compatible con las normas de gestión de riesgos y ciberseguridad en vigencia.

EBIOS RM posibilita la evaluación de riesgos digitales y la identificación de las medidas de seguridad necesarias para su control. Además, permite validar el nivel de riesgo aceptable y avanzar en una perspectiva de mejora continua a largo plazo. Por último, este enfoque brinda recursos y fundamentos valiosos para la comunicación y la toma de decisiones tanto internas como con socios de la organización.[Agence nationale de la sécurité des systèmes d'information (ANSSI),].

3.4.5. Evaluación de riesgos

Hay una amplia gama de enfoques para evaluar el riesgo, algunos más complejos que otros. Sin importar el método que se elija, el resultado debería ser similar.No existe un único mejor enfoque para la selección de una metodología para realizar una evaluación de riesgos; sin embargo, los resultados deben cumplir con las metas y los objetivos de la organización, al identificar la calificación de riesgo relativa de los activos y procesos críticos para la empresa. También es esencial, identificar el máximo riesgo significativo como sea posible. [isa, 2021].

La elección de la metodología, a menos que lo determine la dirección, debería fundamentarse en aquella que se adapte mejor a la organización. [isa, 2021].

La relevancia de NIST y COBIT 5 no se basa únicamente en su antigüedad, sino en su efectividad y adaptación continua a los desafíos tecnológicos y de seguridad. Estos enfoques proporcionan estructuras, estándares y mejores prácticas para abordar riesgos cibernéticos y

de gestión de información, respaldados por el reconocimiento de reguladores e industria. Su capacidad de evolucionar y mantenerse al día con amenazas emergentes los hace valiosos. Aunque hay otros marcos disponibles, la longevidad de NIST y COBIT 5 refleja su utilidad constante como herramientas confiables para una gestión efectiva de riesgos y ciberseguridad.

Método NIST

Esta metodología de evaluación de riesgos incluye 9 pasos primordiales:

1. Caracterización del sistema (o dominio general).
2. Identificación de la amenaza.
3. Identificación de la vulnerabilidad.
4. Análisis de control.
5. Determinación de probabilidad.
6. Análisis de impacto.
7. Determinación de probabilidad.
8. Análisis de impacto.
9. Determinación de riesgos.
10. Recomendaciones de control.
11. Documentación de resultados.

[isa, 2021]

Los pasos 2,3,4, y 6 se pueden realizar en paralelo después de completar el paso 1.
La figura 15 describe estos pasos y las entradas y salidas de cada paso.

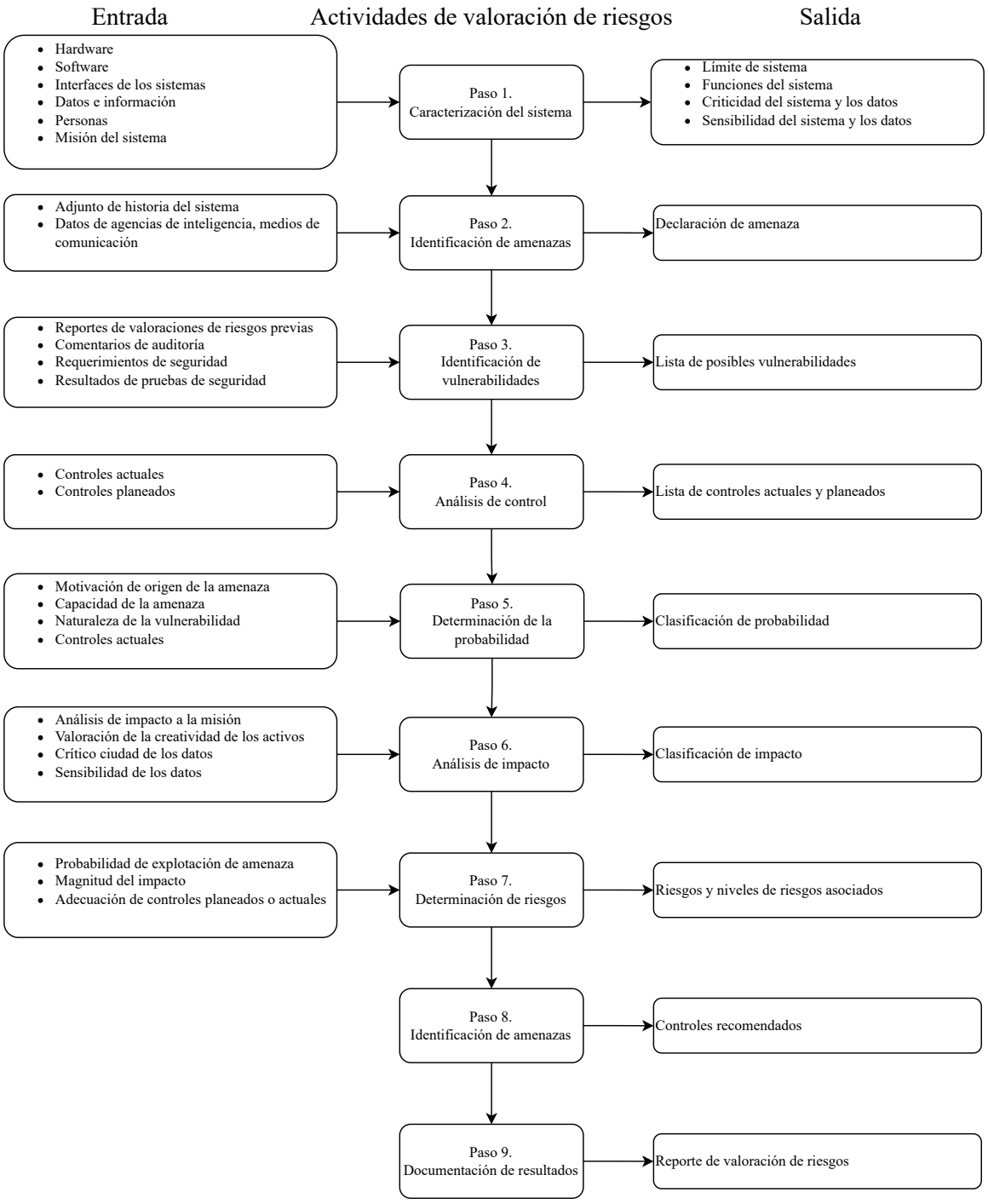


Figura 15: Metodología NIST de análisis de riesgos. Adaptado de [isa, 2021].

Método COBIT 5

Utilizando el enfoque de COBIT 5 para la evaluación de riesgos, que está alineado con ISO/IEC 27005:2011, la evaluación incluye 3 pasos: identificación, el análisis y la valoración (ver figura 16).

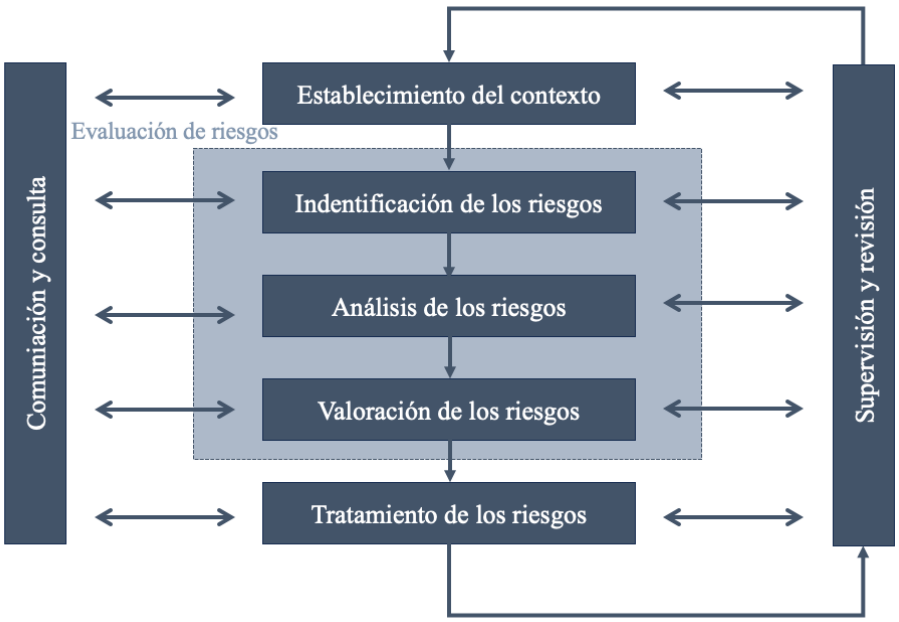


Figura 16: Proceso de gestión de riesgos y fases de la evaluación de riesgos. Adaptado de [isa, 2021]

- La identificación del riesgo es el proceso de utilizar escenarios de riesgos para determinar el rango de la naturaleza del riesgo para la organización, incluye la identificación de:
  - Activos.
  - Amenazas.
  - Vulnerabilidades.
  - Controles existentes.
  - Consecuencias.
- Análisis de riesgos del proceso de combinar la información de la vulnerabilidad recopilada durante una evaluación y la información de amenaza recolectada de otras fuentes para determinar el riesgo de compromiso, tanto en términos de frecuencia como de magnitud potencial, incluye:
  - Evaluación de las consecuencias.
  - Evaluación de la probabilidad de incidentes.
  - Determinación del nivel de riesgo.
- Valoración del riesgo: Se realizan comparaciones entre los niveles de riesgo siguiendo los criterios de evaluación y aceptación de riesgos. Como resultado, se obtiene una lista jerarquizada de los elementos de riesgo y los escenarios de incidentes asociados que dan lugar a dichos elementos de riesgo identificados.

[isa, 2021]

La figura 17 ilustra un enfoque estándar más detallado para la evaluación de riesgos, en el cual el primer paso consiste en ubicar e identificar los activos de información y determinar su valoración. Sin un inventario preciso de los activos, es complicado identificar las vulnerabilidades que podrían ser explotadas por amenazas. Además, es esencial establecer el valor relativo de los activos en términos empresariales, ya que el posible impacto de la pérdida de activos (consecuencias) es un componente clave para la evaluación del riesgo y también para la clasificación.

Si asumimos que el activo tiene un valor significativo, el siguiente paso es determinar si existen vulnerabilidades que puedan conducir a pérdida o daño. Una vez identificadas las vulnerabilidades, es necesario evaluar las amenazas viables. Si el activo tiene tanto valor como vulnerabilidades susceptibles a amenazas viables, entonces existe un riesgo. Para aclarar este punto, las vulnerabilidades para las cuales no existen amenazas viables no representan riesgo en ese momento (aunque las amenazas puedan surgir en el futuro).

Otra perspectiva es que a medida que aumenta el valor de un activo y se incrementa el número de vulnerabilidades asociadas a él, junto con un mayor rango de amenazas viables, el riesgo de pérdida también aumenta. [isa, 2021]

Las siguientes etapa consiste en definir de manera precisa las consecuencias y el impacto, es decir, cómo las amenazas y vulnerabilidades afectan la disponibilidad, integridad y confidencialidad de los activos de información. Una vez que se han evaluado las consecuencias o impactos y se ha estimado la probabilidad de los incidentes relacionados con los activos en cuestión, se contrastarán los resultados obtenidos se contrastarán con los criterios de aceptación de riesgo establecidos.[Instituto Nacional de Ciberseguridad, 2016]

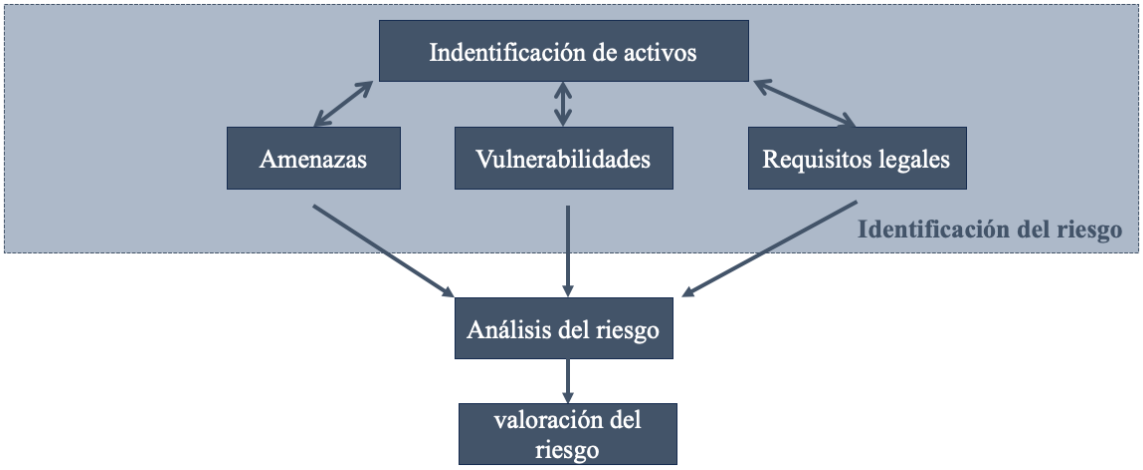


Figura 17: Marco de referencia de análisis de riesgo. Adaptado de [isa, 2021].

Identificación de riesgos

En cualquier organización, corresponde en primer lugar disponer de un inventario y clasificación de activos tecnológicos y de información adecuados. Por lo tanto, el inicio del proceso de evaluación de riesgos involucra la identificación y el registro exhaustivo de todos los activos de información, al mismo tiempo que se establece su valor relativo en términos empresariales.
Se necesita llevar a cabo la categorización de activos de información para determinar la sensibilidad y la importancia relativa de dichos activos, a veces denominada también como el valor

para el negocio.[isa, 2021, Martínez, 2018].

En una organización de tamaño acotado o de muy reciente establecimiento, se puede considerar algo asumible y no muy complicado disponer de un sistema similar, del tipo de las tradicionales CMDB (*Configuration Management Data Base*) o similar. En una organización compleja y de tamaño relevante puede ser una tarea de gran envergadura, ya que es posible que se manejen terabytes o petabytes de datos electrónicos, almacenes de documentos y se involucren miles de personas y dispositivos. Pero es necesario saber qué se tiene para decidir cómo proteger los activos, contra que y por qué.[isa, 2021, Martínez, 2018].

Sin embargo, si no se establece el valor para el negocio, la sensibilidad de los activos de información (y cada vez más en cumplimiento con requisitos legales y regulatorios) se volverá imposible desarrollar un programa de gestión de riesgos efectivo que proporcione una protección adecuada en proporción al valor y sensibilidad de los activos para el negocio y su nivel de importancia. En situaciones en las que no se pueda llevar a cabo una categorización exhaustiva debido a limitaciones de recursos u otras razones, una alternativa menos eficaz podría ser una evaluación de la dependencia del negocio. Esto podría utilizarse como base para distribuir de manera proporcional las actividades de mitigación, centradas en los recursos de información que son esenciales para las áreas críticas de negocio. [isa, 2021].

Una vez que se haya establecido una relación con todos los activos, es fundamental comprender las amenazas que tienen el potencial de ocasionar perjuicios a la información, los procesos y los recursos de soporte. Identificar estas amenazas y evaluar los posibles daños que podrían generar es un proceso que se puede llevar a cabo mediante consultas a los propietarios de los activos, usuarios, expertos y otras fuentes pertinentes. Para cada una de las amenazas analizaremos las vulnerabilidades que puede explotar. La norma ISO 27005 incluye un anexo (ver 9) con ejemplos de vulnerabilidades y amenazas que puede servir de apoyo en esta tarea.[Instituto Nacional de Ciberseguridad, 2016, iso, 2011].

Identificación y valoración de activos

Esta fase es esencial debido a que el valor comercial forma parte del proceso de determinación del riesgo (es decir, el riesgo existe cuando hay una probabilidad de impacto y consecuencias [riesgo = probabilidad × consecuencias]).

El proceso de valoración, que busca homogeneizar los valores en términos financieros, es directo para algunos activos como el hardware, puede valorarse fácilmente en función de los costes de reemplazo. En otros casos, el valor de la información puede reflejar el costo de recrearla o restaurarla, o bien estar relacionado con su contribución a la generación de ganancias. En determinadas situaciones, el valor está ligado a los costos resultantes y las posibles multas derivadas de la exposición de datos privados o de la pérdida de secretos comerciales.[isa, 2021].
En la mayoría de los casos, una evaluación efectiva de los recursos se basa en escenarios de pérdida. Los activos de información pueden ser clasificados y presentados en una matriz (Ver figura 18) que contemple cada posible escenario de pérdida, lo cual ayuda a simplificar un problema complejo y facilita su comprensión.

Escenario	Tipo de Datos	Tamaño de Pérdida	Pérdida de Reputación	Demandas perdidas	Pérdida de Multas/Reg.	Pérdida de Mercado	Pérdida por año esperada	Notas
Intrusos (hackers) roban información y públicamente chantajean a las empresas	Cliente datos	1K registros 10K registros	US $1M US $20M	US $1M US $10M	US $1 US $35M	US $1M US $5M	US $10M	Pérdida regular de la capacidad para realizar adquisiciones por 1 año
Empleados que roban información y la venden a los competidores	Estratégico plan	Plan a 3 años	Mínimo	Mínimo	Mínimo	US $20M	US $2M	Los competidores duplican los nuevos productos, llegan al mercado más rápido
Los contratistas roban información y la venden a los piratas informáticos	Empleados datos	10K registros	US $5M	US $10M	Mínimo	Mínimo	US $200,000	
Las cintas de respaldo y la información que se encontraron en la basura son noticias de primera página	Cliente datos	10M registros	US $20M	US $20M	US $10M	US $5M	US $200,000	

Figura 18: Matriz de escenarios de pérdidas. [isa, 2021]

Las metodologías de valoración de activos de información consideran diversas variables, como el nivel de complejidad técnica y el posible impacto financiero directo y sus consecuencias. En general, las evaluaciones cuantitativas [4] son más precisas, aunque pueden volverse complejas al analizar los efectos reales.
Los activos intangibles generalmente abarcan propiedad intelectual, como secretos comerciales, patentes y derechos de autor, así como la gestión del conocimiento, la reputación de la marca, la cultura corporativa, la lealtad de los clientes y la innovación. Estos activos pueden ser difíciles de cuantificar, por eso se utilizan evaluaciones cualitativas [5](aunque un incidente en sí mismo posiblemente no cause pérdidas directas, los clientes podrían alejarse debido a la falta de confianza en la organización, especialmente si existe una fuerte competencia).[isa, 2021].

Una enfoque sumamente útil consiste en vincular los activos con los servicios tecnológicos proporcionados por la organización.
De esta manera, un conjunto específico de activos de bajo nivel (como servidores, bases de datos, aplicaciones, etc.) se asocia a un servicio de TI (como correo electrónico, navegación web, desarrollo de software, mantenimiento de sistemas, etc.), y estos servicios respaldan procesos de negocio identificados en un mapa de procesos. Esta abstracción desde el detalle hasta la generalidad cumple diversos objetivos: [Martínez, 2018].

- Permite considerar los detalles como un conjunto, agregando los riesgos de bajo nivel a los procesos de negocio de alto nivel. Relaciona activos concretos con lo que realmente importa, es decir, los procesos de negocio que a su vez se han priorizado según la estrategia de la organización.

- A pesar de esta abstracción, el concepto de "servicio de TI" se mantiene a un nivel técnico suficientemente preciso y con una estructura tecnológica definida, lo que permite aplicar

[4]El enfoque cuantitativo implica asignar valores numéricos a diversos aspectos del riesgo, como probabilidades y magnitudes de impacto.
[5]El enfoque cualitativo se basa en descripciones y evaluaciones subjetivas. En lugar de asignar valores numéricos, se utilizan categorías o escalas cualitativas para clasificar el riesgo.

marcos de control de ciberseguridad, desde el fortalecimiento (bastionado) hasta la detección avanzada de amenazas (*threat hunting*) pasando por la detección de comportamientos y el aprendizaje automático (*machine learning*).

[Martínez, 2018].

Sin embargo, este enfoque también conlleva ciertas dificultades que no deben subestimarse:

- La correcta identificación de los activos es una tarea compleja en sí misma. ¿Están todos los activos que deberían estar? ¿Son todos los activos que se encuentran? Esta tarea es esencial para cualquier organización de TI y requiere mantener un inventario actualizado.
- Abstraer riesgos específicos (como una vulnerabilidad crítica en un servidor de base de datos no parcheable debido a su impacto en la aplicación) hacia un servicio de TI y, a su vez, hacia un proceso.
- La gestión basada en procesos puede suponer un desafío, ya que no todas las organizaciones se gestionan de esta manera. Aquellas que optan por este enfoque asumen un reto significativo. Aunque centrarse en el nivel de servicio de TI asegura la primera línea de gobernanza, comprender las operaciones y su sustento, es posible que se vea limitada la aportación de valor real al negocio. No obstante, esto se puede abordar trabajando en colaboración con las unidades de negocio u otras áreas similares. La creatividad y la colaboración pueden ser muy útiles en esta situación.

[Martínez, 2018].

Una vez alcanzado este punto, donde ya se dispone de un inventario aceptable, reconocible y gestionable de activos, una descripción de los "servicios de TI"proporcionados a la organización o directamente a clientes y terceros, y una asignación adecuada de cada activo a esos servicios, se ha construido una base sólida de información y una forma de gestión tecnológica. [Martínez, 2018].

Análisis del riesgo

La fase de análisis de riesgos implica evaluar y comprender tanto la magnitud del riesgo identificado como su naturaleza, junto con las posibles implicaciones del compromiso específico. En esta etapa, también se determina la efectividad de los controles existentes y hasta qué punto pueden mitigar el riesgo identificado. El análisis de riesgo implica: [isa, 2021]

- Análisis exhaustivo de las fuentes de riesgo (amenazas y vulnerabilidades) identificadas en la etapa de identificación de riesgos.
- Creación de escenarios específicos que describen cómo podrían manifestarse las amenazas y cómo podrían interactuar con las vulnerabilidades. Estos escenarios ayudan a comprender mejor los posibles eventos de riesgo y sus consecuencias.
- Asignación de valores numéricos a los diferentes aspectos del riesgo, como la probabilidad y el impacto. Esto puede implicar cálculos cuantitativos para obtener métricas específicas que permitan comparar y priorizar los riesgos.

.

[isa, 2021].

Análisis de las fuentes de riesgos

Dentro de la fase de análisis del riesgo en la gestión de riesgos, se encuentra un enfoque fundamental para comprender y evaluar en detalle los elementos que contribuyen al riesgo de la información: el "análisis de factores de riesgo de la información" (FAIR). Este enfoque estratégico permite descomponer el riesgo y la comprensión de sus componentes (Ver figura 19). El enfoque ofrece un proceso de análisis razonado y detallado además de una perspectiva elaborada para tomar decisiones informadas y definir estrategias de mitigación efectivas. [isa, 2021].

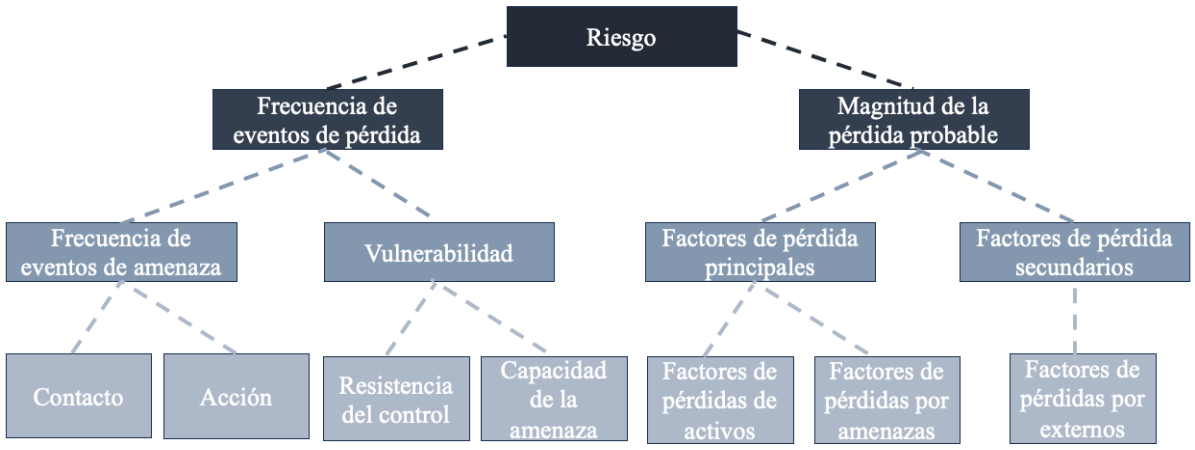


Figura 19: Análisis de factores para el riesgo de información. Adaptado de [isa, 2021]

Elaboración de escenarios de riesgos

Una vez se ha realizado un análisis de las fuentes de riesgo, se debe elaborar un escenario de riesgo. La construcción de escenarios de riesgo implica la descripción de posibles eventos de riesgo y la documentación de los factores y áreas que podrían verse afectados por tales eventos. Estos eventos abarcan desde fallos en el sistema hasta la pérdida de personal clave, robo, interrupciones en las redes, cortes de energía y desastres naturales, así como cualquier otra situación que pueda impactar la misión de las operaciones empresariales. Cada escenario de riesgo debe estar estrechamente relacionado con un impacto en los objetivos comerciales.[isa, 2021].

La clave para desarrollar estos escenarios radica en concentrarse en eventos de riesgo relevantes y plausibles. Algunos ejemplos incluyen la creación de un escenario basado en un cambio drástico en el mercado para los productos de una organización, un cambio en el liderazgo gubernamental o una interrupción en la cadena de suministro. La figura 20 muestra un ejemplo de las diferentes contribuciones que son necesarias para desarrollar escenarios de riesgo. [isa, 2021].

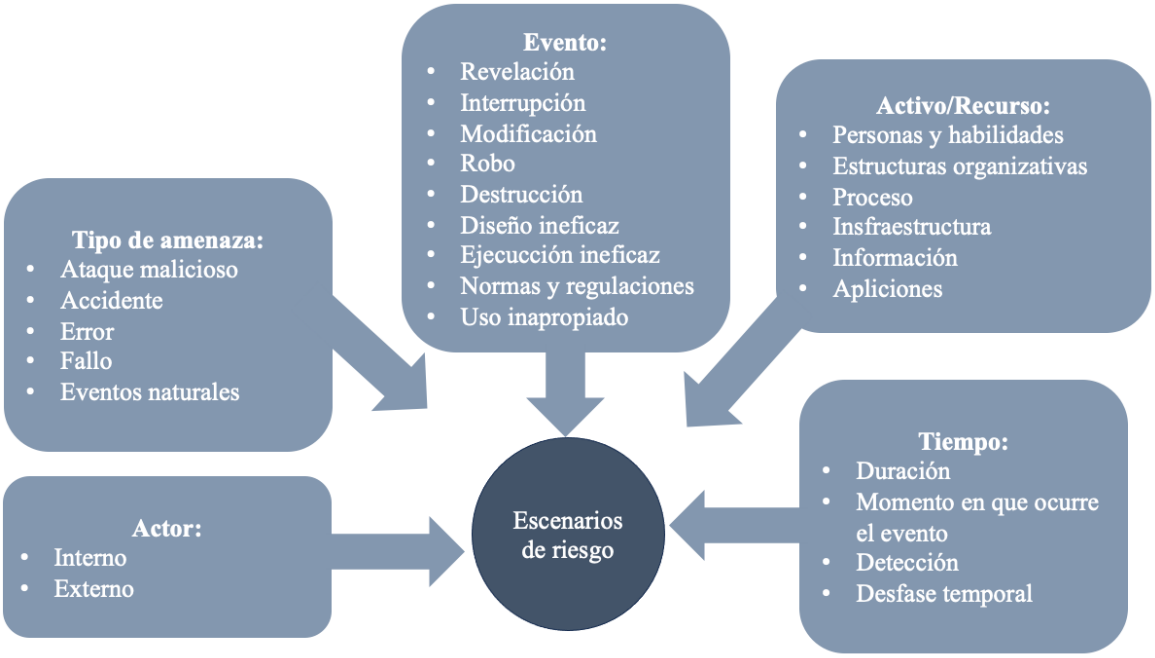


Figura 20: Estructura de escenario de riesgo. Adaptado de [isa, 2021]

Cuantificación del riesgo

Como se ha mencionado previamente, durante la etapa de definición del contexto, se establecen una serie de criterios que actúan como pautas para la evaluación de riesgos. Estos criterios son utilizados para medir las posibles consecuencias o impactos, la evaluación del nivel de riesgo puede ser abordada de diversas formas, como por ejemplo, mediante la utilización de análisis estadísticos y cálculos que integren tanto el impacto como la probabilidad.

Cualquier fórmula o método que combine el impacto y la probabilidad debe estar en línea con los criterios establecidos al definir el contexto de gestión de riesgos. Esto se debe a que un evento puede tener múltiples consecuencias y objetivos diversos, por lo que es esencial combinar las consecuencias y las probabilidades para calcular el nivel de riesgo.
[Instituto Nacional de Ciberseguridad, 2016, isa, 2021].

En casos en los que no se cuenten con datos confiables o relevantes en términos estadísticos (por ejemplo, datos de incidentes almacenados en una base de datos de incidentes), otras estimaciones basadas en factores, como los impactos que han afectado a otras organizaciones, podrían ser realizadas siempre y cuando sean comunicadas y aprobadas de manera adecuada, ya que estas decisiones son fundamentales.

El análisis de riesgos puede variar en su nivel de detalle según el riesgo en cuestión, el propósito del análisis y el grado de protección que los datos, la información y los recursos requieran. Los métodos para realizarla incluyen estimaciones cualitativas y cuantitativas o una combinación de ambas. Suele realizarse una estimación cualitativa inicial para identificar los riesgos que precisan una estimación cuantitativa.. En cualquier caso, el tipo de análisis llevado a cabo debe estar en consonancia con los criterios desarrollados durante la definición del contexto de gestión de riesgos y el consenso alcanzado sobre el enfoque a utilizar, como se mencionó previamente.[Instituto Nacional de Ciberseguridad, 2016, isa, 2021].

- Análisis cualitativo: el análisis cualitativo implica la presentación detallada tanto de la magnitud como de la probabilidad de las posibles consecuencias. Las escalas utilizadas pueden ser creadas o ajustadas según las circunstancias, y distintas descripciones pueden ser aplicadas a diversos riesgos.
  Este enfoque cualitativo puede ser empleado en los siguientes casos: como una evaluación preliminar para identificar riesgos que requieran un análisis detallado adicional, cuando se van a considerar aspectos intangibles del riesgo, como la reputación, la cultura o la imagen de la organización o cuando no se dispone de información adecuada, datos numéricos o recursos necesarios para llevar a cabo un enfoque cuantitativo que sea estadísticamente aceptable.
  Se puede obtener una representación visual común para el análisis cualitativo utilizando una matriz de 5x5, como se ilustra en la figura 21.

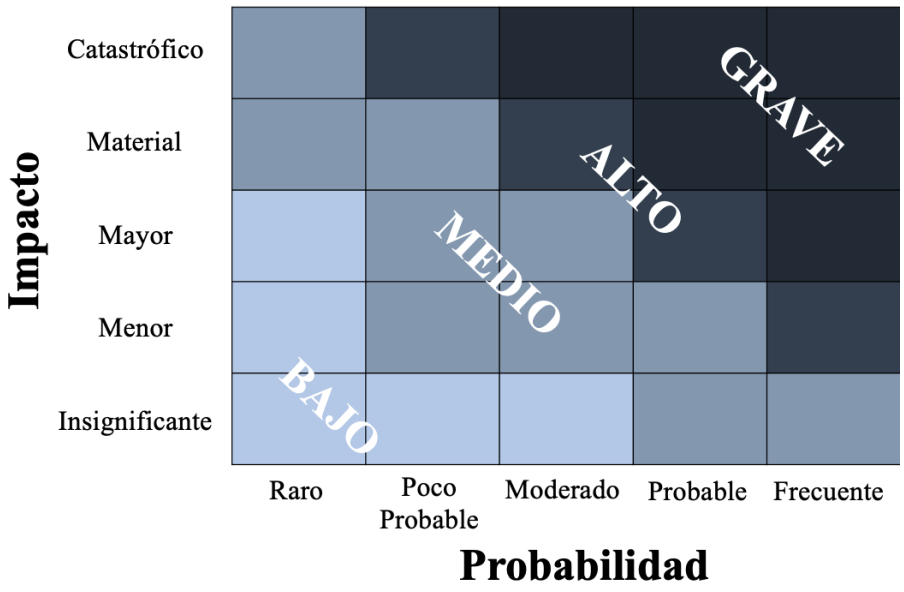


Figura 21: Matriz de impacto semicuantitativo. Adaptado de [ISACA, 2018b]

- Análisis semicuantitativo: el propósito del análisis semicuantitativo es asignar valores a las escalas utilizadas en la evaluación cualitativa. Estos valores tienden a ser representativos más que reales, lo cual es una premisa previa al enfoque cuantitativo. Como resultado, dado que los valores asignados a cada escala no representan con precisión la magnitud real del impacto o la probabilidad, es fundamental que los números se combinen mediante una fórmula que reconozca las limitaciones o suposiciones establecidas en la descripción de las escalas utilizadas.
  Es importante destacar que la aplicación del análisis semicuantitativo puede dar lugar a algunas inconsistencias, ya que los números seleccionados pueden no reflejar adecuadamente las relaciones entre los riesgos, especialmente cuando las consecuencias o la probabilidad son extremas. Para que este enfoque sea efectivo, los valores elegidos deben ser indicativos y suficientes para establecer prioridades entre diferentes riesgos.

- Análisis cuantitativo: en el análisis cuantitativo se asignan valores numéricos tanto al impacto como la probabilidad.

> Éstos valores derivan de diversas fuentes. La calidad de todo el análisis depende de las actitudes, los valores asignados y la validez de los modelos estadísticos utilizados.
> Se puede determinar el impacto mediante la evaluación del proceso de varios resultados de un evento o mediante la extrapolación de estudios experimentales o datos pasados. Tal como aclara el análisis que precede, la especificación del nivel de riesgo no es exclusiva. Tanto el impacto como la probabilidad se pueden expresar o combinar de un modo diferente, de acuerdo con el tipo de riesgo, y el alcance y objetivo del proceso de gestión de riesgos.

[isa, 2021].

En resumen, en la estimación cualitativa se califican las potenciales consecuencias y la probabilidad según niveles (alto, medio, bajo) subjetivos. En la cuantitativa se utiliza una escala con valores numéricos, apoyándose en datos de distintas fuentes por ejemplo incidentes del pasado, experiencia previa, estudios, etc. Cuando el riesgo está cuantificado podremos priorizarlo de manera sencilla, se a partir del supuesto financiero o del valor financiero del activo, y de forma igualmente directa, podemos asociar un cierto retorno económico a la inversión o seguridad necesaria (tendremos una estimación de lo protegido). [Instituto Nacional de Ciberseguridad, 2016, García, 2019].

Evaluación del riesgo

Durante la fase de evaluación de riesgos, se deben tomar decisiones relacionadas con la necesidad de abordar ciertos riesgos y determinar sus prioridades, basándose en el análisis pertinente, considerando margen de error posible dentro de las tolerancias, las cuales pueden ser amplias si no hay datos confiables disponibles.
Si un riesgo cumple con los criterios de aceptabilidad, es probable que la opción de tratamiento sea la aceptación.
Si el riesgo supera el nivel aceptable y no se encuentra dentro de la variación de tolerancia, es más probable que la medida de tratamiento consista en alguna forma de mitigación. Esta fase incluye estas dos subfases:

- Clasificación y priorización de los riesgos identificados. Esto ayuda a determinar qué riesgos son más críticos y necesitan una atención inmediata y cuáles pueden ser gestionados de manera menos intensiva.
- Documentación y registro de todos los riesgos identificados, así como sus características, evaluaciones y prioridades. Este registro servirá como base para la toma de decisiones y la planificación de la mitigación y el tratamiento de los riesgos.

Clasificación y priorización del riesgo

Los resultados obtenidos de la evaluación del riesgo se emplean para establecer un orden jerárquico de riesgos, el cual guía la asignación de esfuerzos para abordarlos. La clasificación de riesgos se deriva de una combinación de todos los elementos que conforman el riesgo, que incluyen la identificación de amenazas, las características y capacidades de la fuente de amenazas, así como la gravedad de las vulnerabilidades y la probabilidad de éxito de un ataque. Esto se realiza teniendo en cuenta la efectividad de los controles existentes, el riesgo de control y el impacto que tendría un ataque exitoso en la organización. Al considerar estos factores en conjunto, se puede determinar el nivel de riesgo asociado con una amenaza en particular.
[isa, 2021].

Por otro lado, la priorización permite a la organización asignar sus recursos y esfuerzos de manera eficiente, enfocándose en los riesgos más significativos y urgentes. Los riesgos de mayor prioridad son aquellos que tienen el potencial de causar el mayor daño o interrupción a la organización, o aquellos que pueden tener un impacto significativo en sus objetivos estratégicos. A medida que se asignan recursos para abordar los riesgos de mayor prioridad, se logra una gestión más efectiva y focalizada de los riesgos, lo que contribuye a la protección y el éxito general de la organización.

El tipo de tablas como la 21 también servirá para estimar qué tratamiento dar a cada riesgo (ver figura 22). Por ejemplo los riesgos que se encuentren la zona roja serán inaceptables pero el resto podemos elegir soportarlos.

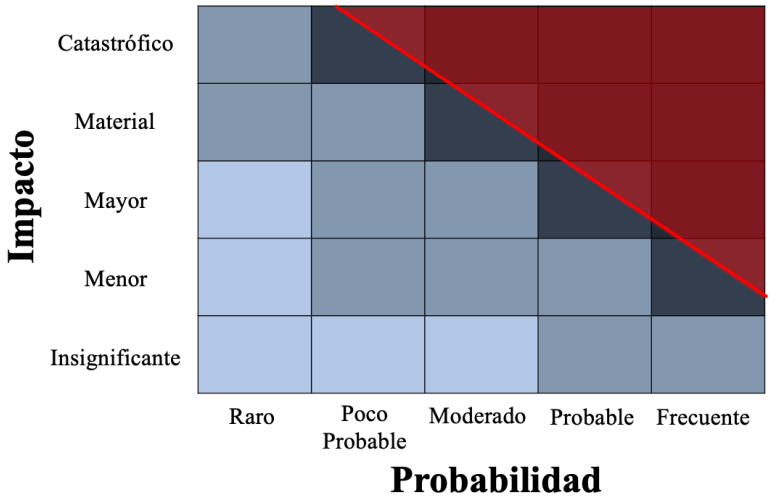


Figura 22: Matriz de impacto para evaluación de riesgos. Adaptado de [ISACA, 2018b] y [Instituto Nacional de Ciberseguridad, 2016].

Registro de riesgos

En el transcurso del proceso de identificación de riesgos y sus componentes, se requiere la creación de un registro de riesgos. Este registro tiene la función de constituir un repositorio centralizado para todos los riesgos relacionados con la seguridad de la información. Esto engloba amenazas específicas, vulnerabilidades, exposiciones y los activos que puedan verse afectados. Dentro del registro, es fundamental detallar la figura del propietario del activo y del propietario del riesgo, así como cualquier otra parte involucrada y con interés en el proceso.

La información contenida en el registro de riesgos debe ser agregada a medida que avance el proceso de evaluación. Una vez que se hayan completado las etapas de identificación, análisis, evaluación y respuesta de los riesgos, y se haya ingresado información relevante en el registro, este se erigirá como un punto de referencia primordial para todas las actividades vinculadas con la gestión de riesgos.

El registro de riesgos constituye una parte esencial del perfil de riesgos de la organización. Un perfil de riesgos es un componente crucial para la eficaz gestión de riesgos de la información. Su función reside en brindar una visión panorámica de los riesgos globales a los que la organización está expuesta, al tiempo que ofrece información relevante y necesaria.

3.4.6. Tratamiento de riesgos

Pasamos a la fase de actuación, fase en la que implantaremos medidas (contra medidas) y controles para reducir (el impacto) de los riesgos.
Como resultado de la fase anterior, se obtendrá una lista de riesgos ordenados o una tabla que los clasifique según su posición. En esta etapa, es necesario decidir cómo abordar cada uno de los riesgos en función de su evaluación y los criterios previamente establecidos. [Instituto Nacional de Ciberseguridad, 2016, García, 2019].

Durante esta fase, se elegirá la opción de tratamiento más apropiada para cada riesgo de la lista. Para tomar esta decisión, se considerará no solo la evaluación obtenida para cada riesgo, sino también el coste asociado con su tratamiento (es necesario poder establecer, para cada una de las actuaciones, su relación coste-beneficio). Por ejemplo, si el coste es considerablemente alto, podría ser más conveniente evitar un riesgo en lugar de mitigarlo. Se dará prioridad a las opciones que ofrezcan una reducción significativa del riesgo de manera económica. El nivel de tolerancia al riesgo se establecerá en función de criterios de coste-beneficio.[isa, 2021, Instituto Nacional de Ciberseguridad, 2016, García, 2019].

El resultado de esta fase se materializa en un plan de tratamiento de riesgos, que implica la elección y justificación de una o varias opciones para cada riesgo identificado. A este plan se agregará una lista de riesgos residuales, es decir, aquellos que aún persisten a pesar de las medidas adoptadas.[Instituto Nacional de Ciberseguridad, 2016]

Frente a la presencia del riesgo, las organizaciones cuentan con cuatro opciones estratégicas:

- Evitar el riesgo: Esto implica poner fin a la actividad que originó el riesgo en primer lugar.
- Transferir el riesgo: Trasladar el riesgo a otra entidad (es importante considerar que la transferencia del riesgo a menudo resulta en la transferencia del impacto).
- Mitigar el riesgo: Implementar medidas y mecanismos de control adecuados para reducir el riesgo.
- Aceptar el riesgo: Reconocer el riesgo y decidir no tomar medidas adicionales para tratarlo.

Es importante destacar que también existe la opción de que una organización decida ignorar el riesgo, lo cual puede ser peligroso. La diferencia radica en evaluar la probabilidad y las consecuencias y determinar si se consideran aceptables dadas las circunstancias. Ignorar el riesgo puede conducir a estimaciones erróneas sobre la probabilidad y el posible impacto, lo que podría resultar en consecuencias graves o desastrosas.

La única situación en la que puede ser prudente ignorar un riesgo es cuando la probabilidad de exposición es extremadamente baja y el impacto es tan excepcionalmente grande y raro que no es factible abordarlo (por ejemplo, la colisión de un meteorito o una guerra nuclear).

Cesar la actividad

Frecuentemente, se presentan oportunidades para modificar las actividades o incluso reestructurar los procesos con el propósito de atenuar o controlar el riesgo hasta alcanzar niveles aceptables.

Un análisis exhaustivo de la actividad podría llevar a la conclusión de que el riesgo no es justificable. En esta situación, es importante destacar que aunque la organización haya decidido detener la producción o el servicio, la responsabilidad persiste mientras el producto o servicio esté en uso.

Transferir el riesgo

Un ejemplo de transferencia de riesgo radica en la decisión que toma una organización de adquirir un seguro para abordar áreas de riesgo. Cuando una entidad adquiere un seguro, parte del riesgo se delega a la compañía aseguradora, a cambio del pago de una prima que refleja la evaluación efectuada por la aseguradora en relación al nivel de riesgo asumido. Es esencial reconocer que el riesgo no se transfiere per se, sino que más bien, el impacto sobre la organización se minimiza a medida que el seguro cubre ciertos o todos los costos asociados a una eventualidad. También es factible transferir riesgos a través de la externalización de funciones, siempre y cuando se establezcan cláusulas de indemnización en los contratos. Sin embargo, cuando se externaliza el riesgo operativo, los acuerdos y convenios con terceros de la empresa deben definir de manera específica las responsabilidades y obligaciones de ambas partes en cláusulas de indemnización particulares.

Los acuerdos de indemnización, que pueden ser parte integrante de un contrato de servicio con proveedores externos, brindan una cierta protección contra posibles incidentes perjudiciales. Aunque es posible traspasar algunos de los posibles impactos financieros relacionados con el riesgo, por lo general no se puede transferir la responsabilidad legal inherente a las consecuencias de cualquier eventualidad.

Mitigar el riesgo

Existen diversas formas de atenuar el riesgo, como por ejemplo, a través de la implementación de mejoras en los controles de seguridad, la aplicación de contramedidas o la modificación de procesos con riesgo. Estos controles pueden ser de naturaleza preventiva y dirigirse directamente al riesgo, o bien pueden enfocarse en reducir la exposición y, por ende, disminuir el riesgo. En ciertos casos, es posible disminuir el riesgo mediante la implementación de contramedidas adecuadas que reduzcan o eliminen una amenaza en particular.
El impacto potencial de un riesgo puede ser reducido mediante la implementación de controles compensatorios, correctivos o a través de procesos técnicos, contractuales o de procedimiento. [isa, 2021].

La puesta en marcha de acciones y controles para mitigar el riesgo es una actividad continuada, y sistematizada, que debe ir haciéndose de forma recurrente sobre todos y cada uno de los activos de nuestra organización. [García, 2019].
Las acciones deben ir en dos líneas de actuación:

1. Primero, reducir la probabilidad del incidente.
2. Segundo, reducir el impacto en caso de éxito.

Normalmente, se trabaja en tres fases:

1. Identificar controles recomendados que, normalmente, reducirán la probabilidad de éxito y el impacto.
2. Realizar un análisis coste-beneficio para cada uno de los controles recomendados.
3. Llevara cabo una priorización de los controles.
4. Diseñar e implementar un plan de acción (un plan mitigación) incluyendo, obviamente, tanto los aspectos de coste como los de tiempo.

[García, 2019].

Controles y contramedidas

Los controles son elementos tecnológicos, procesos, prácticas, políticas, normas o procedimientos diseñados para regular y reducir los riesgos en una actividad determinada.
Dado que es común encontrar una variedad de controles en diferentes etapas de un proceso, es crucial comprender la mitigación de riesgos en su conjunto.[isa, 2021].

Es esencial llevar a cabo la identificación de controles preexistentes para evitar redundancias y costos superfluos, como la duplicación de esfuerzos en la implementación. Además, mientras se identifican estos controles, es recomendable llevar a cabo una revisión para garantizar su correcto funcionamiento. Los controles que se tienen previsto implementar como parte de los planes de tratamiento de riesgo deben ser abordados de la misma manera que aquellos que ya están en funcionamiento. Si un control existente que se planea implementar se considera ineficaz, insuficiente o injustificado, es importante revisarlo cuidadosamente para determinar si es necesario eliminarlo o reemplazarlo con una alternativa más adecuada.
[Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), 2016].

Si bien estratificar controles es sensato, emplear un exceso de controles para el mismo riesgo es ineficiente y suele disminuir la productividad. Además, es esencial evitar que distintos controles se enfrenten al mismo riesgo, lo que invalidaría su estratificación.
Para que las evaluaciones de riesgo sean efectivas y precisas, es fundamental llevarlas a cabo desde el inicio hasta el final de los procesos. Esto permitirá determinar si los controles primarios minimizan o eliminan ciertos riesgos, posiblemente evitando la necesidad de controles posteriores. También ayudará a identificar redundancias y controles duplicados innecesarios.[isa, 2021].
Las categorías de control incluyen las siguientes:

- Preventivos: los controles preventivos tienen como objetivo inhibir los intentos de violación de políticas de seguridad. Estos controles incluyen medidas como la ejecución de control de acceso y la implementación de autenticación, sistemas de defensa (como los cortafuegos, las listas de control de acceso, los procedimientos de revisión de código y de programación segura, las unidades de testeo y control de calidad y seguridad, los controles para mitigar la posibilidad de intrusiones por errores de *buffer overflow*, por vulnerabilidades de formato, o por inyecciones de código o comandos.

- Detectivos: Los controles detectivos identifican las violaciones después de que han ocurrido, ayudan en la identificación de las actividades de un potencial atacante. Estos controles permiten detectar intentos de violación de políticas de seguridad y abarcan aspectos como pistas de auditoría, métodos de detección de intrusos y sumas de verificación.

- Correctivos: los controles correctivos buscan remediar el impacto de una violación, es decir, arreglan y corrigen alguno de los componentes o sistemas después de un incidente. Los procedimientos de respaldo y recuperación son ejemplos de medidas correctivas, ya que permiten restaurar un sistema en caso de que los daños hayan sido significativos y no se pueda continuar operando.

- Compensatorios: los controles compensatorios son mecanismos internos que reducen el riesgo asociado a debilidades existentes o potenciales en los controles, evitando así errores u omisiones.

- Disuasivos: los controles disuasivos emiten advertencias con el propósito de prevenir posibles riesgos. Ejemplos de estos controles incluyen pancartas de advertencia en pantallas de inicio de sesión o incentivos para denunciar intrusos.

[isa, 2021, García, 2019].

Los efectos de los controles se ilustran en la figura 23. Es importante notar que los controles compensatorios y correctivos suelen ser combinados, ya que ambos tratan con el impacto.

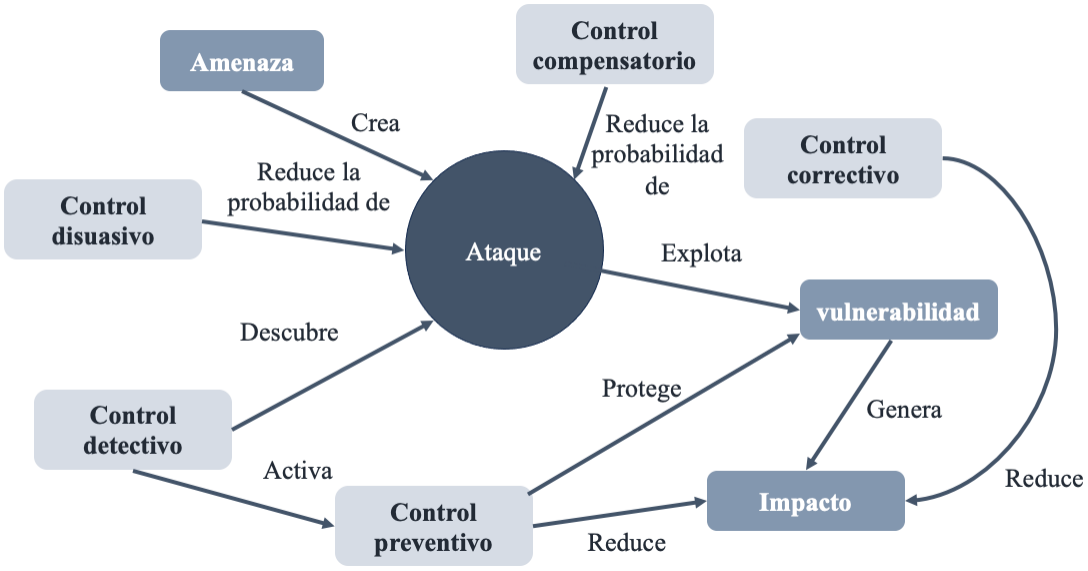


Figura 23: Tipos de controles y sus efectos. Adaptado de [isa, 2021].

Costes y beneficios

Al planificar los controles o contramedidas, una organización debe tener en cuenta los costos y los beneficios de su implementación. Si los costos específicos de los controles o las contramedidas (incluyendo costos indirectos) superan los beneficios de mitigar el riesgo, la organización podría optar por aceptar el riesgo en lugar de asumir los gastos de mitigación. Esto se basa en el principio general de que el costo de un control no debe superar el beneficio esperado. Un análisis de rentabilidad proporciona una visión del impacto financiero de los riesgos y ayuda a determinar cuánto vale la pena invertir para proteger lo que es importante.

Sin embargo, un análisis de costo/beneficio también se relaciona con tomar decisiones informadas, considerando los costos de mitigar riesgos potenciales en comparación con las posibles pérdidas (exposición al riesgo).

Aceptar el riesgo

Existen diversas situaciones en las que es viable aceptar un riesgo específico. Una de ellas es cuando el costo de mitigar el riesgo resulta desproporcionadamente alto en comparación con los beneficios o el valor del activo en cuestión. Sin embargo, es crucial que el proceso de gestión de riesgos de la información permita una documentación precisa y adecuada del riesgo, para que los responsables de la toma de decisiones en el ámbito empresarial puedan optar por aceptar el riesgo con un nivel apropiado de conocimiento y comprensión.

Es importante reconocer que no todos los impactos pueden ser reducidos de manera inmediata, y que las consideraciones pueden ir más allá de consideraciones estrictamente financieras.

Un marco de aceptación de riesgo puede resultar una herramienta valiosa para establecer criterios de aceptación de riesgo y el nivel de gestión en el cual se decide aceptar dicho riesgo.[isa, 2021].

Riesgo residual

Los riesgos que subsisten incluso después de la implementación de controles y contramedidas son conocidos como riesgos residuales. Aunque el riesgo nunca se elimina por completo, siempre persiste en forma residual. Es importante destacar que la reducción de un riesgo inevitable puede dar lugar a la introducción de otro riesgo, que esperamos sea de menor magnitud. El objetivo radica en asegurar que el riesgo residual se alinee con los criterios de tolerancia al riesgo aceptables establecidos por la organización. La tolerancia al riesgo se define como la variación permisible del riesgo aceptable y, por lo general, se expresa en forma de porcentaje.[isa, 2021].

El objetivo es garantizar que el riesgo residual sea equivalente a los criterios de la organización para el riesgo aceptable y la tolerancia a riesgos. La tolerancia al riesgo se define como la desviación permitida del riesgo aceptable y, por lo general, se describe como porcentaje o rango. El riesgo residual aceptable también debe ser el resultado de cumplir con los objetivos de control definidos y será equivalente a los niveles mínimos de seguridad definidos para la organización. [isa, 2021].

Después de revisar los distintos enfoques de tratamiento de riesgos en el proceso de gestión de riesgos, es importante proporcionar una guía clara sobre cuándo utilizar cada tipo de tratamiento. En la siguiente figura, se detallan las circunstancias en las que conviene aplicar cada estrategia de tratamiento, basándose en 24a un análisis de coste-beneficio y 24b evaluación del impacto y la probabilidad asociados a cada riesgo. Tanto la tabla como la figura servirán como referencia práctica para tomar decisiones informadas sobre cómo abordar los riesgos de manera eficiente y efectiva, asegurando que los recursos se asignen de manera óptima para proteger los activos y objetivos clave de la organización.

Coste-beneficio	Tratamiento
El coste del tratamiento es muy superior a los beneficios	Evitar el riesgo
El coste del tratamiento es adecuado los beneficios	Mitigar el riesgo
El coste del tratamiento por terceros es más beneficiosos del tratamiento directo	Transferir el riesgo
El nivel de riesgo está muy alejado del nivel de tolerancia	Aceptar el riesgo

(a) Análisis coste-beneficio.Adaptado de [isa, 2021].

(b) Evaluación impacto-probabilidad. Adaptado de [García, 2019].

Figura 24: Ejemplo criterios para el tratamiento de riesgos.

4. Metodología

Como se ha destacado en el inicio, la gestión de riesgos constituye una faceta fundamental y al mismo tiempo amplia dentro del ámbito de la seguridad de la información. Dado su alcance, este trabajo se focaliza en un aspecto específico de esta disciplina: la identificación y valoración de riesgos. El enfoque elegido responde a la intención de resolver una problemática actual, que se relaciona con la falta de uniformidad en la representación de activos. Esta situación se manifiesta en la diversidad de formatos, nombres y otros atributos que presentan los activos, lo cual puede dificultar su análisis cohesivo y efectivo en términos de riesgo. Por tanto, el propósito es abordar este desafío y lograr una unificación de activos que permita una gestión más eficiente y precisa de los riesgos asociados a la seguridad de la información.

En el mundo de la seguridad de la información, no puedes proteger algo si no sabes que existe. Por eso, la gestión de activos de ciberseguridad es un componente crítico para la base de las operaciones de ciberseguridad en todo tipo de empresas, sin conocer con certeza qué existe en la infraestructura de TI de la empresa, resulta complicado determinar dónde se encuentran los riesgos más graves y asignar recursos de seguridad de manera eficiente.
Al permitir que tu equipo de seguridad mantenga un directorio en tiempo real de activos de tecnología de la información, así como los riesgos de seguridad asociados, la gestión de activos de ciberseguridad es fundamental para lograr un enfoque "de toda la empresa.[en] una estrategia de seguridad proactiva y completa de extremo a extremo. [Ordr, 2023].

Cualquier dispositivo, recurso o servicio que exista dentro de tu infraestructura de tecnología de la información podría estar sujeto a riesgos o vulnerabilidades que puedan dar lugar a una brecha en el recurso individual y en tu red en su conjunto, en caso de que los atacantes utilicen un recurso comprometido como punto de entrada para llevar a cabo un ataque más amplio.
Es por esto por lo que la gestión de activos de ciberseguridad desempeña un papel fundamental al proporcionar a los equipos de seguridad y a las empresas una visión completa y actualizada de los recursos de TI y los riesgos asociados. Esto permite construir estrategias de seguridad sólidas que puedan abordar de manera proactiva las amenazas, lo que a su vez conlleva importantes ventajas.[Ordr, 2023].

Además, la gestión de activos de ciberseguridad posibilita una respuesta proactiva a las amenazas. Al monitorear continuamente la infraestructura de TI en busca de nuevos riesgos y despliegues, los equipos de seguridad no necesitan esperar a detectar un ataque activo para tomar medidas. Pueden identificar y abordar las amenazas antes de que se conviertan en problemas graves. Asimismo, en caso de que ocurra un ataque, la gestión de activos de ciberseguridad proporciona a los equipos de seguridad un inventario actualizado de activos y riesgos. Esto les permite comprender rápidamente lo que salió mal y cuándo. En lugar de tener que reconstruir la configuración de recursos y despliegues para investigar el origen de una brecha, los equipos tienen un registro detallado al que pueden acceder de inmediato.[Ordr, 2023]

Por otro lado, la falta de una gestión adecuada de activos de ciberseguridad o su implementación deficiente conlleva riesgos significativos para las empresas. Uno de los riesgos más destacados es la mayor probabilidad de interrupciones comerciales. Cuando una brecha afecta a datos o sistemas críticos, la empresa puede quedar paralizada, lo que no solo daña su reputación, sino que también tiene graves consecuencias financieras.

Finalmente, una gestión ineficaz de activos también limita la capacidad de los equipos de seguridad para operar eficazmente. La falta de un listado preciso de recursos y riesgos dificulta la automatización de las operaciones de seguridad, lo que obliga al equipo a buscar y asegurar dispositivos manualmente, lo cual es una ineficiencia en términos de tiempo y recursos financieros.[Ordr, 2023].

En el proceso de gestión de activos, se ha optado por emplear la metodología EBIOS (Evaluación de los Riesgos y la Información de los Sistemas, por sus siglas en francés) desarrollada por la Agencia Nacional de Ciberseguridad de Francia (ANSSI) para llevar a cabo la identificación de activos. La elección de EBIOS se fundamenta en su exhaustividad y solidez en comparación con las metodologías de identificación de activos como COBIT 5 y NIST, además, es importante mencionar que la metodología EBIOS cuenta con la recomendación y respaldo de la ENISA, la Agencia de la Unión Europea para la Ciberseguridad.

Mientras que EBIOS es respaldada por una agencia europea, tanto el Instituto Nacional de Estándares y Tecnología (NIST) como el Marco de Control para la Gobernanza de Tecnologías de la Información (COBIT) son enfoques desarrollados en los Estados Unidos. La elección de EBIOS como metodología puede estar relacionada con una preferencia por un marco que esté más alineado con las necesidades y regulaciones europeas en materia de ciberseguridad, garantizando así un enfoque adaptado a las condiciones específicas de la región.

EBIOS ha demostrado ser una metodología integral y robusta en el ámbito de la ciberseguridad y la gestión de riesgos. Ofrece un enfoque estructurado y detallado para identificar activos y evaluar los riesgos asociados a ellos. Su enfoque desde los más altos niveles hasta las funciones técnicas, junto con su capacidad para generar escenarios de riesgo estratégicos y operativos, lo convierte en una opción valiosa para abordar la identificación de activos de manera completa.
Si bien COBIT 5 y NIST son marcos reconocidos en la ciberseguridad y gestión de riesgos, su enfoque en la identificación de activos puede ser más limitado en comparación con EBIOS. Este último brinda una mayor amplitud y profundidad en el proceso de identificación, lo que nos permite obtener una visión más completa y precisa de los activos involucrados en nuestro contexto específico.[de Gobierno Electrónico y Sociedad de la Información y del Conocimiento., 2021].

La evaluación de riesgos de este trabajo usa la escala de evaluación ISO 27005, una escala del 0 al 4 que sigue las pautas establecidas en el estándar ISO 27005, donde 0 representa el riesgo más bajo y 4 el riesgo más alto. Este estándar es una referencia ampliamente aceptada para la gestión de riesgos en el ámbito de la seguridad de la información. En este contexto, la evaluación de riesgos se realiza con esa escala de acuerdo a la cultura específica de la empresa.

4.1. Activos

Como se ha mencionado anteriormente, en el ámbito de la seguridad de la información, la identificación y clasificación de activos es un paso fundamental para garantizar una gestión efectiva de los riesgos. La Agencia Nacional de Ciberseguridad de Francia (ANSSI) ha desarrollado una metodología robusta y completa conocida como EBIO, que destaca por su enfoque exhaustivo en la identificación de activos. Esta metodología no solo se centra en la identificación de los activos en sí, sino que también abarca la comprensión profunda de su valor, uso y relaciones dentro del entorno organizativo. Al adoptar esta metodología, las organizaciones pueden superar el desafío de la unificación de activos, asegurando que los activos se identifiquen de manera consistente, con un formato uniforme y un lenguaje compartido en todos los niveles de la empresa.

Es importante destacar que la Agencia Europea de Ciberseguridad (ENISA) recomienda y respalda la metodología EBIOS desarrollada por ANSSI. Esta recomendación de ENISA subraya la eficacia y la relevancia de la metodología EBIOS en el contexto de la ciberseguridad y la gestión de activos de información. Al seguir las directrices y las mejores prácticas establecidas por EBIOS, las organizaciones pueden fortalecer significativamente su postura de seguridad cibernética y mejorar su capacidad para identificar, evaluar y proteger activos críticos en un mundo digital en constante evolución.

Así, por tanto, los activos pueden agruparse en diferentes categorías siguiendo la metodología EBIOS (Ver figura 25), lo que facilita la organización y clasificación de estos elementos críticos. Esta categorización se basa en criterios específicos que abarcan no solo la naturaleza de los activos, sino también su importancia estratégica y su contribución al funcionamiento de la organización. La adopción de esta clasificación detallada no solo permite una gestión más efectiva de los activos, sino que también promueve una comprensión más profunda de su relevancia en el contexto operativo de la empresa, lo que a su vez facilita la toma de decisiones informadas en materia de seguridad cibernética. Este enfoque integral contribuye a una estrategia de gestión de riesgos más sólida y a una mejor protección de los activos de información críticos.

Supporting asset	Examples (incomplete list)
Information and telephone systems	
Hardware	
User terminal	Computer, laptop, tablet, mobile phone
Peripheral device	Printer, scanner, keyboard, mouse, camera, microphone, connected object
Telephone	Fixed or mobile phone, analogue or IP
Storage equipment	USB key, hard drive, CD-ROM, memory card
Server	Mainframe, blade server, rack server
Means of administration	Administration station, administration tool servers, bastion
Telephone	Switch, router, inbound gateways from outside, Wi-Fi terminal
Storage equipment	Firewall, intrusion detection system (IDS/IPS), VPN gateway
Server	Programmable logic controller, sensor, actuator, SCADA system, safety instrumented system
Software	
Infrastructure service	Directory service, IP address management service (DHCP), domain name service (DNS), domain controller, print server
Application/application service	Web server, web service, application server, email server, database server, software packages (HR, customer relations, ERP
Middleware	Enterprise Application Integration (EAI), Extract-Transform-Load (ETL), Open DataBase Connectivity (ODBC)
Operating system (OS), hypervisor	Windows, Linux, MacOS, Xen
Firmware	Basic Input Output System (BIOS), Unified Extensible Firmware Interface (UEFI), mobile phone component manager, program stored in a USB key equipped with a microprocessor
Security software	Security Information and Event Management (SIEM)
Networks/computer and telephone channel	
Network/computer channel	Network cable, fibre optic, radio link (Wi-Fi, Bluetooth, etc.)
Network/telephone channel	Telephone line
Organisations	
Individual	Employee, trainee, service provider, maintenance personnel
Paper document	Handwritten or printed document
Verbal exchange	Meeting, informal exchange
Social engineering element	Information shared over the social networks
Physical installations and premises	
Site/building/room	Head office, plant, storage site, industrial building, meeting room, server room
Physical security system	Access systems by badge, intrusion detection system, video-protection system

Figura 25: Tipos de activos según ANSII. Adaptado de [Agence nationale de la sécurité des systémes d'information (ANSSI),].

Después de haber completado el proceso de listar los activos potenciales en una empresa, el enfoque de este trabajo se dirigirá hacia dos componentes críticos aplicaciones e infraestructura (los equipos). Estos incluyen tanto los servidores como las máquinas de usuario, conocidas como *workstations* (ws), y es aquí donde surge un desafío considerable en términos de la correcta gestión de activos.

Los servidores, que desempeñan un papel fundamental en la administración y almacenamiento de datos y aplicaciones, son piezas esenciales de la arquitectura tecnológica de una organización. Por otro lado, las *workstations* son las herramientas principales de trabajo de los empleados, brindando un acceso directo a los recursos y datos empresariales. Sin embargo, es común que se presenten dificultades a la hora de mantener un inventario preciso de estos equipos, ya que a menudo se les asignan diferentes nombres en diversas fuentes de información, como bases de datos, hojas de cálculo de Excel, escaneos de red, entre otros.

Esta discrepancia en los nombres y fuentes de información puede llevar a la falta de coherencia en la gestión de activos y a la dificultad para tener una visión integral y precisa de la infraestructura tecnológica. Esto se traduce en riesgos potenciales de seguridad, ineficiencia en la administración y la incapacidad para tomar decisiones informadas sobre la protección de los activos tecnológicos.

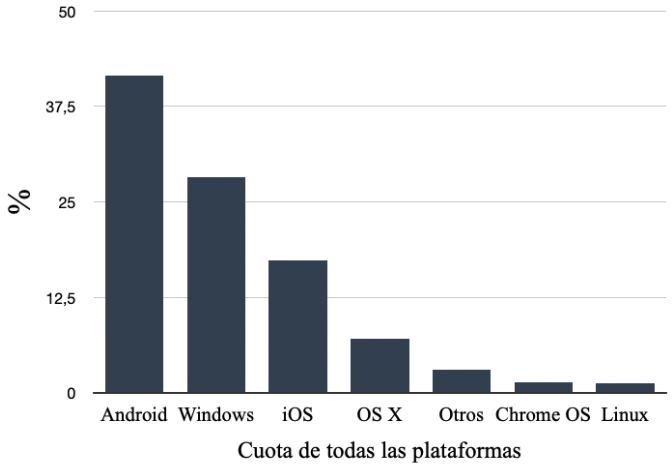
Los sistemas operativos, por su parte, son el corazón de cualquier dispositivo informático, determinando su funcionamiento y capacidades. En este contexto, es crucial identificar los sistemas operativos presentes en cada servidor y *workstation*, así como sus versiones y configuraciones específicas. Esto no solo ayuda a comprender la infraestructura tecnológica en detalle, sino que también proporciona información vital para la gestión de parches, actualizaciones y seguridad.

Además de los sistemas operativos, también es fundamental considerar los programas informáticos que se ejecutan en estos equipos. Los programas y aplicaciones que forman parte del entorno tecnológico de una organización desempeñan un papel crucial en la funcionalidad diaria y en la realización de tareas específicas. Desde herramientas de productividad hasta aplicaciones especializadas, estos programas agregan valor a los activos tecnológicos.

Cuota de mercado de los S.O. actuales

Cuando se evalua el panorama general de los sistemas operativos, considerando todas las plataformas disponibles, los datos de marzo de 2023 proporcionados por "*Statcounter*"nos revelan que Android se destaca como el sistema operativo líder (ver figura 26). En resumen, Android domina con un 41.56 % de cuota, seguido por Windows, iOS y otros sistemas operativos en el panorama de dispositivos y plataformas de ese periodo.

Si tenemos en cuenta que Android y Chrome OS, son Linux, podemos concluir que Linux domina el mercado con un margen enorme.[WebLinus, 2023].



- Android: 41.56 %
- Windows: 28.29 %
- iOS: 17.29 %
- OS X: 7.00 %
- Otros: 3.05 %
- Chrome OS: 1.32 %
- Linux: 1.17 %

Figura 26: Cuota de todas las plataformas. Adaptado de [WebLinus, 2023].

Analizando las cosas por partes:

S.O en servidores

En el ámbito de los servidores, Linux y el software libre ejercen un dominio innegable. De acuerdo con datos proporcionados por "W3Techs", un 33.5 % de los servidores web funcionan con "Nginx", mientras que un 31.5 % emplea .ªpache". Estos servidores se ejecutan sobre plataformas LAMP o LEMP (Linux, Nginx o Apache, MySQL y PHP). Por su parte, "Microsoft-IISrepresenta el 6 % del mercado en este segmento.

En lo que respecta a los servidores de correo electrónico, prevalece la presencia de Linux. "Sendmail"lidera con un 30.3 %, seguido de .ªximçon un 19.4 % y "Postfixçon un 14.2 %, sumando un impresionante 63.9 % en cuota de mercado para Linux. En contraste, Microsoft cuenta con un 21.7 % de participación, mientras que otros sistemas aportan un 14.5 %.

En cuanto a los servidores DNS, "bind.es la opción dominante en sistemas Linux, con un 77 %. Microsoft se sitúa en un segundo lugar con un 10 %, y otros sistemas representan un 13 %, según datos de "dns.measurement-factory.com".[WebLinus, 2023].

En un contexto amplio, en lo que concierne a los sistemas operativos de los servidores, Linux y Unix se posicionan como líderes, abarcando el 81 %, en contraposición al 19 % de utilización de Windows (ver figura 27). Este hecho resalta de manera significativa la predominancia de Linux y el software de código abierto en el entorno de los servidores.

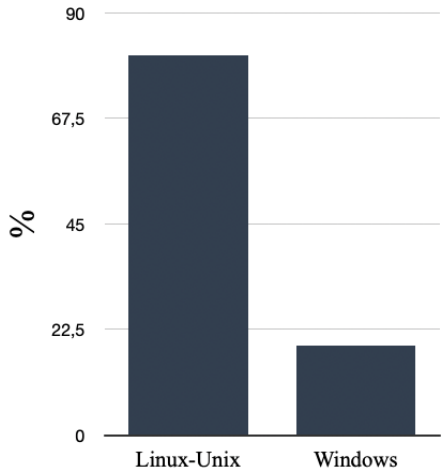


Figura 27: S.O en servidores. Adaptado de [WebLinus, 2023].

SO en workstation

Cuando analizamos la cuota de mercado de los sistemas operativos en entornos de escritorio, es innegable que Windows continúa manteniendo su posición predominante. Esto se debe en gran medida a la práctica común de vender equipos con Windows preinstalado y a que la garantía a menudo depende de mantener este sistema operativo.

De acuerdo con los datos proporcionados por "Statcounter", aunque con una tendencia a la disminución, el sistema operativo de Microsoft aún ostenta una cuota de mercado del 69.43 %. Le sigue OS X con un 17.2 %, otros sistemas con un 7.26 %, Chrome OS con un 3.24 %, Linux con un 2.86 % y FreeBSD con un 0.01 %.

Si comparamos estos datos con los de 2018, que eran los siguientes: Windows 76.17 %, OS X 12.33 %, otros sistemas 8.46 %, Chrome OS 1.35 % y Linux 1.69 %, podemos observar claramente la tendencia a la disminución de la cuota de mercado de Windows y el aumento en la cuota de mercado de todos los demás sistemas operativos de escritorio. (ver figura 28.)

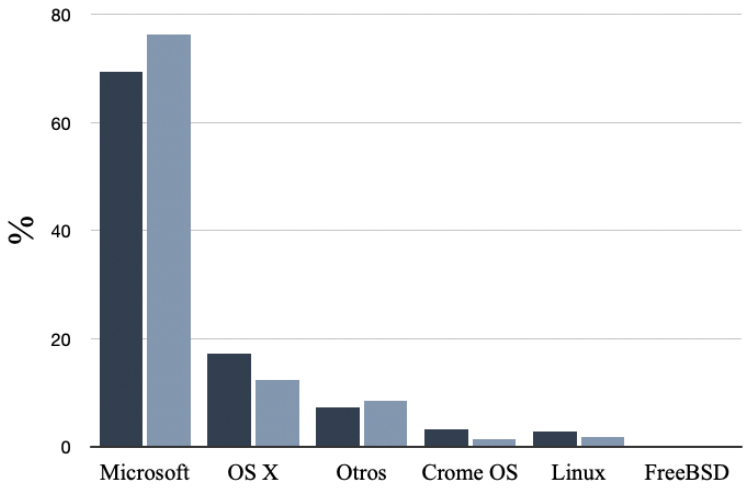


Figura 28: Evolución de S.O. en los últimos 5 años. Adaptado de [WebLinus, 2023].

Volviendo a a la identificación y valoración de riesgos, la gestión de programas informáticos puede ser compleja, ya que, al igual que con los equipos y sistemas operativos, la diversidad de fuentes y nombres puede generar dificultades en la identificación y unificación. La correcta catalogación de los programas, su versión y la relación con los sistemas operativos en uso se convierten en elementos esenciales para una gestión eficaz de activos tecnológicos y para garantizar la seguridad y la continuidad de las operaciones.

En este contexto, la identificación y unificación de los nombres y atributos de los equipos, así como la centralización de la información en un sistema único y confiable, son esenciales para abordar el desafío del inventario de activos de manera efectiva. Al superar esta dificultad, las organizaciones pueden contar con una base sólida para la evaluación de riesgos y la toma de decisiones informadas en relación con la seguridad de la información y la gestión de activos tecnológicos.

Como se ha explicado anteriormente, para proponer una identificación y valoración de los riesgos, la ENISA (Agencia de la Unión Europea para la Ciberseguridad) recomienda el uso del marco (EBIOS) desarrollado por la ANSII (*National Cybersecurity Agency of France*). Este marco proporciona pautas claras sobre qué información se debe recopilar acerca de los activos para lograr un control efectivo de los mismos en el contexto de la ciberseguridad.

La información requerida deriva de la guía titulada "MAPPING THE INFORMATION SYSTEM How-to guide in 5 steps"(Mapeo del Sistema de Información: Guía de cómo hacerlo en 5 pasos) [of France, 2023]. En el Anexo III de este trabajo, se puede encontrar el Apéndice I de esta guía, que incluye tablas completas de información relevante que se debe considerar sobre los activos para un correcto inventario. Sin embargo, para este proyecto en particular, se ha seleccionado únicamente la información de las líneas correspondientes a los activos que se utilizarán (aplicaciones e infraestructura). Específicamente, se han considerado algunas líneas de las tablas de las vistas (view) 3, 5 y 6 (del Anexo).Ver figuras 30 y 29. Se ha excluido el resto de la información del Anexo, ya sea porque está fuera del alcance de este trabajo o porque no compete para los objetivos específicos del proyecto. [of France, 2023].

OBJECT	ATTRIBUTE
Logical server	Identification (identifier, IP address, MAC address) and description
	Technical characteristics: model, OS and version
	Active network services
	Physical support server
	Linked applications
Physical server	Identification: identifier, IP address, DNS name
	Technical characteristics: type, model, OS and version
	Physical location: site, building, room, bay
	Logical server(s) attached
	Operations Manager

Figura 29: Información sobre activos (Servidores) . Adaptado de [of France, 2023].

OBJECT	ATTRIBUTE
Application unit	Identification and description
	Manager
Application	Identification and description
	List of using entity(ies)
	Entity responsible for operations
	Cybersecurity manager
	Type of technology: thick-client, Web, etc.
	Type of application: internal development, software, software package, script, EAI/ESB platform, etc.
	Volume of users and profiles
	Security requirements (CIAT)
	External exposure (e.g. Software as a Service – SaaS type solution)
	List of logical servers supporting the application

Figura 30: Información sobre activos (App) . Adaptado de [of France, 2023].

La tabla 29 proporciona una estructura organizada para recopilar información crucial sobre los servidores tanto lógicos como físicos. La información detalla es:

Para servidores lógicos:

- Identificación: Esto incluye el identificador único del servidor, su dirección IP, y dirección MAC, junto con una descripción que lo identifique de manera clara.
- Características técnicas: Se refiere al modelo del servidor, su sistema operativo y la versión del sistema.
- Servicios de red activos: Esto involucra cualquier servicio de red que esté actualmente en funcionamiento en el servidor.
- Servidor de soporte físico: Si el servidor lógico está vinculado a un servidor físico específico, esta información se debe registrar aquí.
- Aplicaciones vinculadas: Si este servidor lógico tiene aplicaciones vinculadas, es importante registrarlas para comprender las relaciones entre los activos.

Para servidores físicos:

- Identificación: Esto abarca el identificador único del servidor físico, su dirección IP y nombre DNS.

- Características técnicas: Incluye el tipo de servidor, modelo, sistema operativo y versión.
- Ubicación física: Esta sección detalla la ubicación física del servidor, que puede incluir el sitio, edificio, sala y posición en el rack.
- Servidor(es) lógico(s) adjunto(s): Si este servidor físico está conectado a uno o varios servidores lógicos, se deben registrar aquí.
- Gestor de Operaciones: En esta sección, se puede registrar cualquier información relacionada con el software o sistema utilizado para la gestión de operaciones del servidor.

La tabla 30 por el contrario, se centra en recopilar información esencial relacionada con las aplicaciones en una organización. Aquí se describen los atributos clave que se deben registrar para cada unidad de aplicación y aplicación individual:

Para la unidad de aplicación:

- Identificación y descripción: Esto incluye un identificador único y una descripción clara de la unidad de aplicación en cuestión.
- Gerente: El responsable de la unidad de aplicación se registra aquí.

Para la aplicación individual:

- Identificación y descripción: Similar a la unidad de aplicación, se proporciona un identificador único y una descripción para cada aplicación individual.
- Lista de entidades que utilizan la aplicación: Aquí se enumera qué entidades o partes dentro de la organización hacen uso de la aplicación.
- Entidad responsable de las operaciones: Indica qué parte o entidad de la organización es responsable de las operaciones de la aplicación.
- Gerente de ciberseguridad: El gerente encargado de la ciberseguridad de la aplicación se registra en esta sección.
- Tipo de tecnología: Describe la tecnología subyacente utilizada por la aplicación, como si es una aplicación de cliente pesado ("thick-client"), basada en web, etc.
- Tipo de aplicación: Esto especifica el tipo de aplicación, ya sea desarrollo interno, software, paquete de software, script, plataforma EAI/ESB (Integración de Aplicaciones Empresariales / Bus de Servicio Empresarial), etc.
- Volumen de usuarios y perfiles: Indica cuántos usuarios hacen uso de la aplicación y qué perfiles de usuario existen.
- Requisitos de seguridad (CIAT): Se refiere a los requisitos de seguridad críticos, es decir, los niveles de confidencialidad, integridad, disponibilidad y trazabilidad que deben mantenerse para la aplicación.
- Exposición externa: Si la aplicación tiene una exposición externa, por ejemplo, si es una solución tipo Software como Servicio (SaaS), se registra en esta sección.

- Lista de servidores lógicos que respaldan la aplicación: Se incluyen los servidores lógicos que son esenciales para el funcionamiento de la aplicación.

Esta información es fundamental para comprender completamente las aplicaciones en el entorno de la organización, identificar responsabilidades, evaluar los riesgos de seguridad y garantizar que las aplicaciones se utilicen y gestionen de manera efectiva y segura.

Esta información es esencial para un inventario completo de activos y una valoración de riesgos efectiva. Permite a las organizaciones comprender completamente sus activos, identificar relaciones y dependencias entre ellos y, en última instancia, tomar decisiones informadas sobre cómo protegerlos en el contexto de la ciberseguridad.

Se debe recordar que en el contexto de la gestión de riesgos y ciberseguridad, los activos de una organización están estrechamente relacionados con una serie de factores críticos que influyen en su seguridad y protección.
La conectividad a Internet desempeña un papel importante en la exposición de los activos a las amenazas cibernéticas. Los activos que están conectados a Internet pueden ser más susceptibles a ataques cibernéticos y amenazas en línea. Por lo tanto, es crucial evaluar cuidadosamente qué activos están conectados a la red y cómo se conectan. Además, en este contexto, la naturaleza de las direcciones IP asociadas a estos activos es un aspecto crítico, la dirección IP asociada a un activo (pública o privada) puede influir en su visibilidad y accesibilidad desde Internet, lo que tiene implicaciones en su seguridad.

Una dirección IP pública es una etiqueta única asignada a un dispositivo o red que está directamente conectado a Internet. Esta dirección es visible y accesible desde la red global de Internet. Las direcciones IP públicas tienen un propósito fundamental: identificar y enrutar datos de manera efectiva hacia y desde dispositivos en Internet. Por ejemplo, los servidores web, servicios en línea y sitios web utilizan direcciones IP públicas para que los usuarios de Internet puedan acceder a ellos sin problemas.

En contraste, una dirección IP privada es una etiqueta utilizada en una red local o privada, como una red doméstica o empresarial. A diferencia de las direcciones IP públicas, estas direcciones son únicas solo dentro de la red local y no son accesibles directamente desde Internet. Su función principal es identificar dispositivos dentro de la red local y facilitar la comunicación interna. Las direcciones IP privadas permiten que varios dispositivos se conecten a Internet a través de una única dirección IP pública utilizando técnicas de enrutamiento de red, como el NAT (*Network Address Translation*).

Las direcciones IP públicas son más visibles en Internet y, por lo tanto, pueden ser objetivos para escaneos y ataques. Las direcciones IP privadas, por otro lado, se utilizan en redes locales y no son directamente accesibles desde Internet. La gestión adecuada de las direcciones IP, la segmentación de redes y la implementación de medidas de seguridad son esenciales para proteger los activos conectados a Internet.

4.2. Vulnerabilides

Como se ha explicado anteriormente, los activos en un entorno de ciberseguridad pueden estar sujetos a vulnerabilidades. Estas vulnerabilidades son debilidades o fallos en los activos

que podrían ser explotados por amenazas o atacantes para comprometer la integridad, disponibilidad o confidencialidad de la información o los recursos protegidos. Identificar y comprender estas vulnerabilidades es fundamental para la gestión efectiva de la seguridad de la información y la mitigación de riesgos cibernéticos.

Las vulnerabilidades que afectan a los activos suelen estar registradas en un glosario conocido como *Common Vulnerabilities and Exposures* (CVE, por sus siglas en inglés). Es un proyecto de seguridad centrado en software de lanzamiento público, financiado por la División de Seguridad Nacional de EEUU y mantenido por MITRE Corporation; una organización sin fines de lucro que opera centros de investigación y desarrollo financiados con fondos federales en Estados Unidos. El glosario CVE utiliza el Protocolo de automatización de contenido de seguridad (SCAP) para recopilar información sobre vulnerabilidades y exposiciones de seguridad, catalogarlas de acuerdo con varios identificadores y proporcionarles ID únicos. Sin embargo, vale la pena señalar que MITRE no es el único. Los CVE pueden recibir su identificación numérica de las autoridades de numeración comercial (no gubernamentales) que enumerarán las vulnerabilidades y exposiciones encontradas en sus propios productos.[MITRE Corporation, 1999].

Una vez que se publica una entrada de CVE, se incluye el número de identificación (con el formato "CVE-2023-1234567"), una descripción breve de la exposición o el punto vulnerable, y las referencias, las cuales pueden contener enlaces a recomendaciones e informes sobre el punto vulnerable. Esta identificación permite una comunicación clara y efectiva sobre las vulnerabilidades entre profesionales de seguridad, empresas y la comunidad en general. Varios días después de la publicación en la base de datos de vulnerabilidades de MITRE, la Base de Datos Nacional de Vulnerabilidades (NVD) publica el CVE con un análisis de seguridad correspondiente.[MITRE Corporation, 1999, Red Hat,].

Los números de identificación de CVE se asignan a las fallas que cumplen con este conjunto específico de criterios:

1. Se pueden solucionar de forma independiente: la falla puede solucionarse independientemente de las demás.

2. El proveedor afectado las confirma o las documenta: el proveedor de software o hardware reconoce la falla, así como su impacto negativo en la seguridad. O bien, la persona que notificó el punto vulnerable compartió un informe sobre él donde se demuestra que tiene un impacto negativo y que infringe la política de seguridad del sistema afectado.

3. Afectan una base del código.:las fallas que afectan a más de un producto obtienen CVE distintos. En los casos de bibliotecas, protocolos o estándares compartidos, se asigna un solo CVE a la falla si no hay manera de utilizar el código compartido sin quedar expuesto al punto vulnerable. De lo contrario, se asigna un CVE única a cada producto o base de código afectados.

[Red Hat,].

CVE fue lanzado en 1999 por la corporación MITRE para identificar y categorizar vulnerabilidades en software y firmware. CVE proporciona un diccionario gratuito para que las organizaciones mejoren su seguridad cibernética. Antes de que se iniciara CVE en 1999, era muy difícil compartir datos sobre vulnerabilidades en diferentes bases de datos y herramientas. Cada proveedor mantuvo su propia base de datos, con su propio sistema de identificación y diferentes

conjuntos de atributos para cada vulnerabilidad. CVE garantiza que cada herramienta pueda intercambiar datos con otras herramientas, al tiempo que proporciona un mecanismo mediante el cual se pueden comparar diferentes herramientas, como los escáneres de vulnerabilidades.
Si bien algunos pueden cuestionar si la divulgación pública de vulnerabilidades facilita que los piratas informáticos exploten esas vulnerabilidades, en general se acepta que los beneficios superan los riesgos. CVE incluye solo vulnerabilidades y exposiciones conocidas públicamente. Esto significa que los piratas informáticos podrían tener acceso a datos relacionados con el CVE, ya sea que esté en la lista de CVE o no.[MITRE Corporation, 1999].

MITRE define la lista CVE como un glosario o diccionario de vulnerabilidades y exposiciones disponibles públicamente, en lugar de una base de datos y, como tal, está destinada a servir como una línea de base de la industria para comunicarse y dialogar en torno a una vulnerabilidad determinada. Según la visión del MITRE, la documentación CVE es el estándar de la industria mediante el cual avisos de seguridad dispares, rastreadores de errores y bases de datos pueden obtener una línea de base uniforme con la que "hablar" entre sí, comunicándose y deliberando sobre la misma vulnerabilidad en un "lenguaje común".[MITRE Corporation, 1999].

Tradicionalmente, han existido bases de datos públicas que permiten la descarga actualizada de Common Vulnerabilities and Exposures (CVE) o proporcionan Application Programming Interfaces (APIs) que permiten consultar información sobre vulnerabilidades, por ejemplo el sitio web cve.org. Estas bases de datos públicas suelen seguir ciertos protocolos y procesos antes de hacer pública una vulnerabilidad.

En el este trabajo, se ha utilizado una base de datos privada (servicio de pago). Lo que diferencia a estas bases de datos privadas de las públicas es una característica clave: su política de divulgación de vulnerabilidades. A diferencia de las bases de datos públicas (que generalmente no publican una vulnerabilidad hasta que se ha encontrado y verificado una solución efectiva para la misma), las bases de datos privadas a menudo notifican sobre la existencia de una vulnerabilidad incluso antes de que se haya encontrado una solución definitiva para la misma. Esto significa que proporcionan información sobre la vulnerabilidad en una etapa temprana, a menudo tan pronto como se descubre, permitiendo a las partes interesadas tomar medidas proactivas para mitigar el riesgo.

Esta diferencia en la divulgación puede ser valiosa en situaciones en las que es crucial conocer la existencia de una vulnerabilidad lo antes posible, incluso si aún no existe una solución oficial. Esto permite a las organizaciones tomar medidas preventivas, como aplicar parches temporales, implementar controles de seguridad adicionales o tomar otras medidas para reducir la exposición al riesgo hasta que se disponga de una solución definitiva.

A menudo, las vulnerabilidades se evalúan utilizando el Sistema de Puntuación de Vulnerabilidades Comunes (CVSS, del inglés *Common Vulnerability Scoring System*). Es un framework abierto y universalmente utilizado que establece unas métricas para la comunicación de las características, impacto y severidad de vulnerabilidades que afectan a elementos del entorno de seguridad IT. Asigna una puntuación numérica a las vulnerabilidades para evaluar su gravedad. Las puntuaciones CVSS oscilan entre 0,0 y 10,0. Cuanto mayor sea el número, mayor será el grado de gravedad. Cada CVE recibe una puntuación CVSS, que indica su gravedad de seguridad. La clasificación de gravedad de la seguridad ayuda a los desarrolladores y a los equipos de seguridad, a determinar cómo abordar la vulnerabilidad y cuándo.[MITRE Corporation, 1999, INCIBE-CERT, 2023].

CVSS se compone tres grupos principales de métricas (conjunto de variables y valores que se utilizan para cuantificar y evaluar las características de una vulnerabilidad de seguridad): Base, Temporal y de Entorno (Environmental). Cada uno de estos grupos se compone a su vez de otro conjunto de métricas. [INCIBE-CERT, 2023].

- Grupo Base: Engloba las cualidades intrínsecas de una vulnerabilidad y que son independientes del tiempo y el entorno. Las métricas evaluadas en este grupo son:
  - Access Vector (AV). Valores: [L,A,N] (Local, Adjacent, Network.
  - Access Complexity (AC). Valores [H,M,L] (High, Medium, Low).
  - Authentication (Au). Valores [M,S,N] (Multiple, Single, None).
  - Confidenciality Impact (C) . Valores [N,P,C] (None, Partial, Complete).
  - Integrity Impact (I). Valores [N,P,C] (None, Partial, Complete).
  - Availability Impact (A). Valores [N,P,C] (None, Partial, Complete).
- Grupo Temporal: Características de la vulnerabilidad que cambian en el tiempo. Se aplican tres métricas:
  - Exploitability (E). Valores: [U,POC,F,H,ND] (Unproven, Proof-of-Concept, Functional Exploit, High, Not Defined).
  - Remediation Level (RL). Valores: [OF,TF,W,U,ND] (Official Fix, Temporary Fix, Workaround, Unavailable, Not Defined).
  - Report Confidence (RC). Valores: [UC,UR,C,ND] (Unconfirmed, Uncorroborated, Confirmed, Not Defined).
- Grupo Environmental: Las características de la vulnerabilidad relacionadas con el entorno del usuario. En este caso los factores que se evalúan son:
  - Collateral Damage Potential (CDP). Valores: [N,L,LM,MH,H,ND] (None, Low, Low Medium, Medium High, High, Not Defined).
  - Target Distribution (TD). Valores: :[N,L,M,H,ND] (None, Low, Medium, High, Not Defined).
  - Security Requirements (CR, IR, AR). Valores: [L,M,H,ND] (Low, Medium, High, Not Defined).

[INCIBE-CERT, 2023].

Una vez asignados los valores de cada métrica se aplicarán unas fórmulas [6] recogidas en las especificaciones del CVSS y que resultarán en un valor numérico entre 0.0 y 10.0 para cada grupo. Este resultado numérico total puntúa y determina cuantitativamente el impacto final de una vulnerabilidad. El valor numérico final se acompaña de una cadena de texto, denominada vector donde se especifica con la sintaxis (métrica:[valor]) (cada grupo de métricas evaluado. [INCIBE-CERT, 2023].

La utilización del CVE y el CVSS es esencial para mantenerse informado sobre las últimas amenazas cibernéticas y para tomar medidas proactivas para mitigar los riesgos. Los administradores de sistemas y las organizaciones pueden utilizar los CVE IDs para buscar información

[6] Se pueden consultar en: https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator/equations

detallada sobre las vulnerabilidades específicas que afectan a sus activos y utilizar las puntuaciones CVSS para evaluar su gravedad. Esto facilita la identificación y la implementación de soluciones, como parches o actualizaciones de seguridad, que son fundamentales para mantener una postura de seguridad cibernética sólida.

4.3. Power BI

Para llevar a cabo un inventario de riesgos efectivo y, por consiguiente, lograr una identificación y valoración adecuada de los mismos, se ha optado por utilizar Power BI como plataforma principal para nuestro *Dashboard* (panel de control) de gestión. Power BI ofrece una serie de características y ventajas que lo convierten en una elección destacada en este proceso.

Power BI es una colección de servicios de software, aplicaciones y conectores que funcionan conjuntamente para convertir orígenes de datos sin relación entre sí en información coherente, interactiva y atractiva visualmente. Sus datos podrían ser una hoja de cálculo de Excel o una colección de almacenes de datos híbridos locales y basados en la nube.Power BI permite conectarse con facilidad a los orígenes de datos, visualizar y descubrir qué es importante y compartirlo con cualquiera o con todos los usuarios que desee. [Microsoft, ceso].

En primer lugar, Power BI nos permite consolidar y visualizar datos relacionados con riesgos de manera eficiente. Con sus avanzadas capacidades de visualización de datos, podemos representar la información de manera clara y accesible a través de gráficos e informes interactivos, facilitando así la comprensión y análisis de los riesgos presentes en nuestra organización.

La versatilidad de Power BI se refleja en su capacidad para integrar datos de diversas fuentes, lo que nos permite centralizar toda la información pertinente en un solo lugar. Esto simplifica el proceso de identificación de riesgos al proporcionar una visión completa y actualizada de la situación en tiempo real.

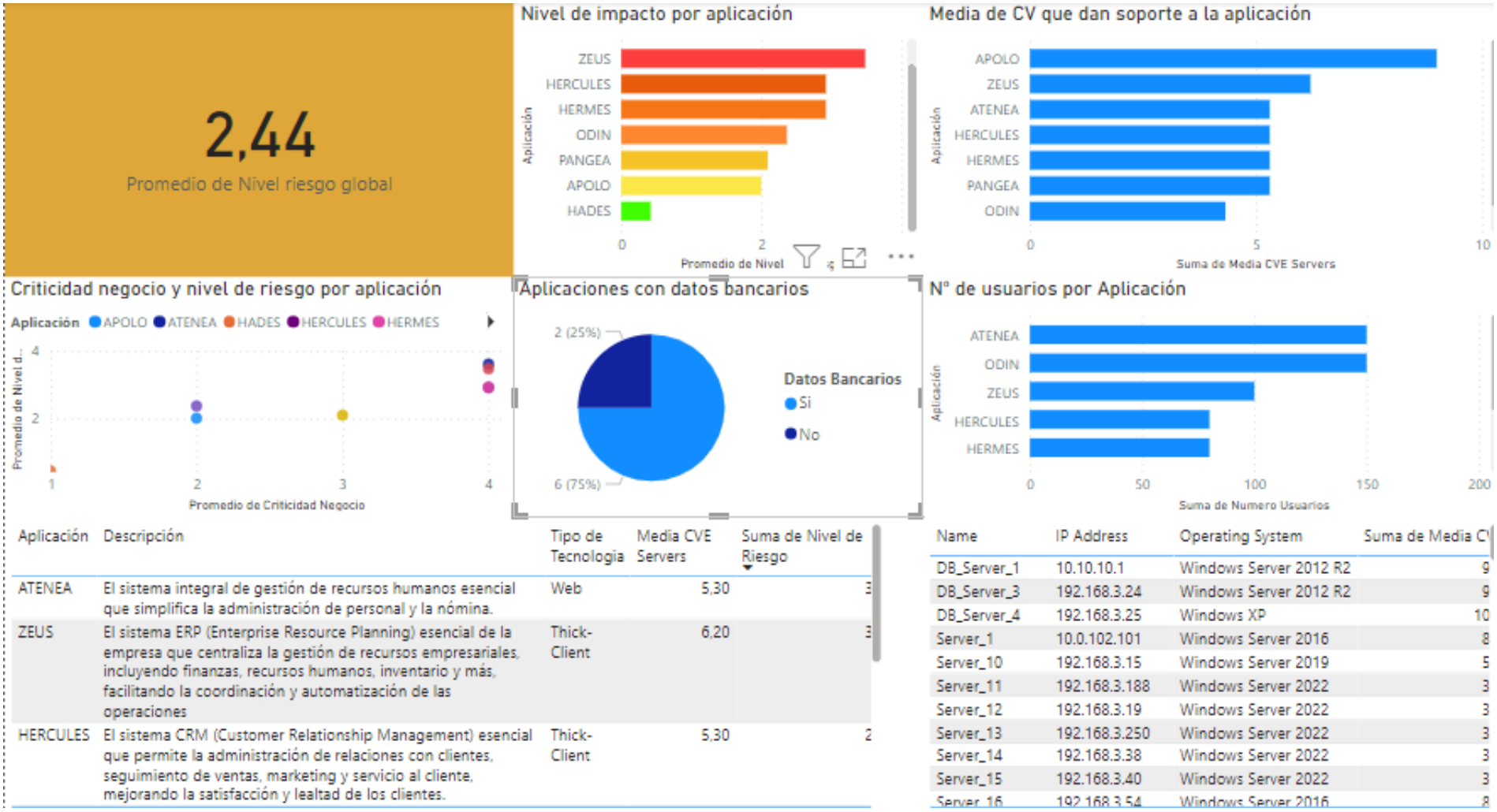
También ofrece la posibilidad de analizar datos en tiempo real, lo que es esencial para mantener nuestros informes y paneles actualizados constantemente. Esto es particularmente valioso en un entorno donde los riesgos pueden evolucionar rápidamente, permitiéndonos tomar decisiones basadas en datos siempre actualizados.

La interactividad que proporciona Power BI mediante la filtración y exploración de datos permite a los usuarios concentrarse en áreas específicas de riesgo y profundizar en detalles según sea necesario. Además, la capacidad de configurar alertas y notificaciones nos ayuda a estar al tanto de cualquier cambio significativo en los indicadores de riesgo. [Microsoft, ceso, Arimetrics, 2023].

Tras haber proporcionado una descripción de esta herramienta, se procede a ilustrar su funcionamiento mediante un *Dashboard*. En concreto, se presentará de manera más detallada una muestra de datos que ha unificada, cruzada y sometida a un proceso de ofuscación o anonimización. El propósito es brindar una comprensión más completa de cómo esta técnica se aplica en la práctica y cómo puede contribuir a la protección de la privacidad y la seguridad de los datos.

4.3.1. *Dashboard*

El *Dashboard* consta de dos páginas principales: una dedicada a las aplicaciones y otra a los activos. Estas dos páginas ofrecen una vista organizada y específica de información relevante para la gestión y supervisión de las actividades de una organización o sistema en particular.



Aplicación	Descripción	Tipo de Tecnologia	Media CVE Servers	Suma de Nivel de Riesgo
ATENEA	El sistema integral de gestión de recursos humanos esencial que simplifica la administración de personal y la nómina.	Web	5,30	3
ZEUS	El sistema ERP (Enterprise Resource Planning) esencial de la empresa que centraliza la gestión de recursos empresariales, incluyendo finanzas, recursos humanos, inventario y más, facilitando la coordinación y automatización de las operaciones	Thick-Client	6,20	3
HERCULES	El sistema CRM (Customer Relationship Management) esencial que permite la administración de relaciones con clientes, seguimiento de ventas, marketing y servicio al cliente, mejorando la satisfacción y lealtad de los clientes.	Thick-Client	5,30	2

Name	IP Address	Operating System	Suma de Media CV
DB_Server_1	10.10.10.1	Windows Server 2012 R2	9
DB_Server_3	192.168.3.24	Windows Server 2012 R2	9
DB_Server_4	192.168.3.25	Windows XP	10
Server_1	10.0.102.101	Windows Server 2016	8
Server_10	192.168.3.15	Windows Server 2019	5
Server_11	192.168.3.188	Windows Server 2022	3
Server_12	192.168.3.19	Windows Server 2022	3
Server_13	192.168.3.250	Windows Server 2022	3
Server_14	192.168.3.38	Windows Server 2022	3
Server_15	192.168.3.40	Windows Server 2022	3
Server_16	192.168.3.54	Windows Server 2016	8

Figura 31: Dashboard aplicaciones.

En la página de aplicaciones se proporciona información detallada sobre las aplicaciones utilizadas por la organización. Esto incluye:

Descripción de las aplicaciones

Aplicación	Descripción	Tipo de Tecnologia	Media CVE Servers	Suma de Nivel de Riesgo
ATENEA	El sistema integral de gestión de recursos humanos esencial que simplifica la administración de personal y la nómina.	Web	5,30	
ZEUS	El sistema ERP (Enterprise Resource Planning) esencial de la empresa que centraliza la gestión de recursos empresariales, incluyendo finanzas, recursos humanos, inventario y más, facilitando la coordinación y automatización de las operaciones	Thick-Client	6,20	
HERCULES	El sistema CRM (Customer Relationship Management) esencial que permite la administración de relaciones con clientes, seguimiento de ventas, marketing y servicio al cliente, mejorando la satisfacción y lealtad de los clientes.	Thick-Client	5,30	

Figura 32: Dashboard: Descripción de las aplicaciones.

Según se ve en la figura 32, se proporciona información sobre las aplicaciones que elegidas en este muestreo, el número de aplicaciones fundamentales que una empresa suele tener puede variar considerablemente según el tamaño de la empresa, su industria y sus necesidades específicas. Sin embargo, algunas aplicaciones fundamentales suelen ser:

- Sistema ERP (*Enterprise Resource Planning*): este sistema centraliza la gestión de recursos empresariales, incluyendo finanzas, recursos humanos, inventario, compras y más. Es fundamental para la coordinación y automatización de las operaciones.
- CRM (*Customer Relationship Management*): Un sistema CRM ayuda a administrar las relaciones con los clientes, el seguimiento de ventas, el marketing y el servicio al cliente. Mejora la satisfacción y lealtad de los clientes.
- Sistema de Gestión de Recursos Humanos: facilita la administración de personal, la gestión de nóminas y otros procesos relacionados con recursos humanos.
- Herramientas de Comunicación y Colaboración: Esto incluye herramientas de correo electrónico, software de colaboración en equipo y soluciones de videoconferencia, que son esenciales para la comunicación interna y externa.
- Sistema de Gestión de Contenido: para la creación, almacenamiento y gestión de documentos y contenidos.
- Aplicaciones de Seguridad Informática: Herramientas de seguridad, antivirus, firewalls y sistemas de gestión de amenazas para proteger los activos digitales.
- Aplicaciones de Comercio Electrónico: Si la empresa vende productos en línea, una plataforma de comercio electrónico es fundamental.
- Herramientas de Analítica de Datos: Para el análisis de datos y la toma de decisiones basadas en datos.

En este muestreo en concreto las aplicaciones son: ZEUS, ODIN, APOLO, HERMES, HÉRCULES, ATENEA, PANGEA y HADES.

Las columnas que se han usado en la muestra para desarrollar la información de las aplicaciones son:

- Aplicación: El nombre de la aplicación en cuestión.
- Descripción: Una breve descripción de la función y el propósito de la aplicación.
- Manager: el nombre del gerente o responsable de la aplicación.Se ha usado un nombre por defecto.
- CyberManager: el nombre del gerente de ciberseguridad o responsable de la seguridad de la aplicación. Se ha usado un nombre por defecto.
- Tipo de Tecnología**: el tipo de tecnología utilizada para desarrollar la aplicación, como "Thick-Client"(cliente pesado) o "Web"(aplicación web). Una aplicación SaaS (Software as a Service), que se ejecuta en la nube, puede ser más difícil de gestionar en términos de ciberseguridad en comparación con una aplicación Thick-Client (cliente pesado) que se instala en el propio ordenador de la empresa. Aunque SaaS es más conveniente en algunos aspectos, puede ser más desafiante gestionar la seguridad debido a la dependencia de terceros y la exposición constante a la web.
- Tipo de Aplicación: el tipo de aplicación, que puede ser Ïnternal development"(desarrollo interno) o "Software"(software de terceros).
- Número de Usuarios**: La cantidad de usuarios que utilizan la aplicación.
- Exposición**: una indicación de la exposición de la aplicación al riesgo, con valores que pueden variar en función de la evaluación de riesgos de la organización.
- Criticidad Negocio: una medida de la importancia de la aplicación para el negocio, con valores que pueden variar en función de la evaluación de riesgos de la organización.
- Nivel de Riesgo: el nivel de riesgo asociado a la aplicación, con valores que pueden variar en función de la evaluación de riesgos de la organización.
- Media CVE Servers: una medida relacionada con las vulnerabilidades conocidas de los servidores que ejecutan la aplicación, con valores específicos que indican la gravedad de estas vulnerabilidades.
- Datos Bancarios: indica si la aplicación maneja o almacena datos bancarios ("Sí.º "No"). Saber si una aplicación contiene datos bancarios es esencial para la gestión de riesgos en ciberseguridad porque ayuda a identificar áreas críticas que requieren una atención especial en términos de seguridad, cumplimiento normativo y respuesta a incidentes.

Para más información sobre esta sección consultar el Anexo III

Promedio de nivel de riesgo global

Figura 33: Dashboard:Promedio de nivel de riesgo global.

A la hora de calcular el riesgo, si se ha optado por el análisis cuantitativo, el riesgo corresponde a la ecuación:

RIESGO = PROBABILIDAD x IMPACTO

Una vez obtenido el impacto de cada aplicación, se calculará el impacto total haciendo la media de los impactos de las aplicaciones individuales. Y se multiplicará por la posibilidad de que ocurra un evento no deseado, como una vulnerabilidad que sea explotada con éxito por un atacante. Esta probabilidad debe basarse en una evaluación específica de las amenazas y vulnerabilidades para el entorno particular de la organización.

La escala de riesgo de la empresa como se ha comentado está basada en la ISO 27005, donde 0 es el mínimoo nivel de riesgo y 4 el máximo:

Figura 34: Escala de riesgo.

Media de CV por aplicación

Como se ha comentado anteriormente, el CVE se utiliza para identificar y etiquetar las vulnerabilidades específicas, cada CVE tiene asociado un CVSS, que se utiliza para evaluar y puntuar la gravedad de esas vulnerabilidades. Estas puntuaciones se aplican a las vulnerabilidades individuales, para calcular el impacto de un conjunto de vulnerabilidades en una aplicación, se puede hacer la media de las puntuaciones de CVSS de esas vulnerabilidades. Esto te da una idea general de la gravedad promedio de las vulnerabilidades que afectan a la aplicación y por tanto del impacto.

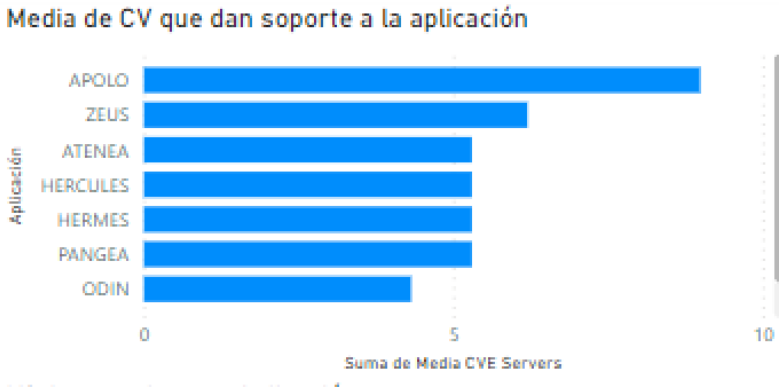


Figura 35: Dashboard: Media de CV por aplicación.

En esta muestra, es la aplicación APOLO la que tiene la media más alta de CVSS.

Nivel de impacto por aplicación

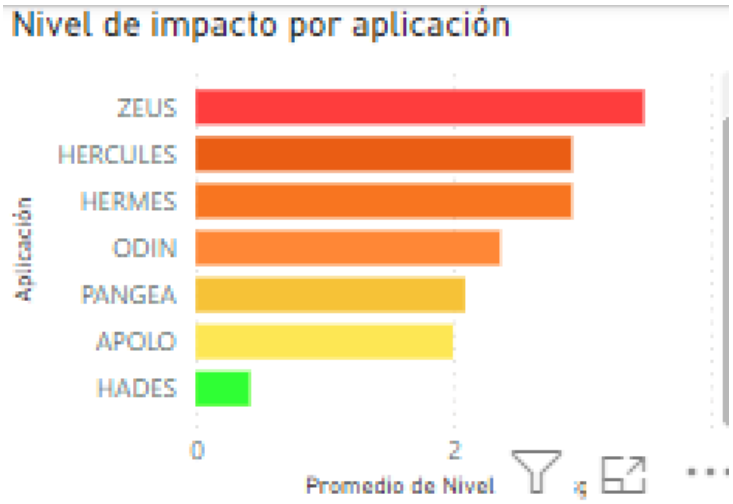


Figura 36: Dashboard: Nivel de impacto por aplicación.

Como se ha comentado anteriormente, el CVSS proporciona información sobre el impacto potencial de una vulnerabilidad. Para calcular el impacto de manera efectiva, no sólo se debe considerar la media de CVSS de las CVE de las aplicaciones, si no también se tener en cuenta la experiencia del equipo de seguridad, los datos específicos del negocio y la importancia de la aplicación para la organización. Al ponderar la media de CVSS por la importancia para el negocio, se puede obtener una evaluación más precisa del impacto de las vulnerabilidades en el contexto de la empresa.

La experiencia del de seguridad y el historial de incidentes previos son factores importantes para evaluar el impacto. Si la organización tiene experiencia en la gestión de incidentes de seguridad o ha enfrentado problemas similares en el pasado, esta experiencia puede ayudar a determinar cómo las vulnerabilidades podrían impactar tus operaciones y activos.

Además, la importancia de la aplicación para el negocio es crucial. Se debe considerar cómo crítica es la aplicación para las operaciones de la empresa. Esto incluye factores como la disponibilidad de la aplicación, la confidencialidad de los datos que maneja y su papel en los procesos comerciales fundamentales. La pérdida de acceso o la exposición de datos confidenciales pueden tener un impacto significativo en la continuidad del negocio y la reputación.

Para calcular por tanto el impacto de manera más precisa, se ha ponderado la media de CVSS de las vulnerabilidades por la importancia de la aplicación para el negocio. Esto significa que las aplicaciones críticas para el negocio tendrán un mayor peso en el cálculo del impacto que las aplicaciones menos críticas. Esta ponderación refleja mejor el impacto real de las vulnerabilidades en las operaciones.

Criticidad de negocio y nivel de impacto por aplicación

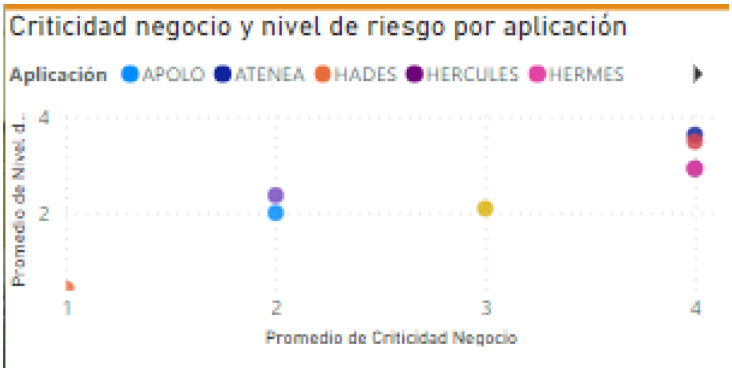


Figura 37: Dashboard: Criticidad de negocio y nivel de impacto por aplicación.

Tener un diagrama de dispersión que compare el nivel de impacto por aplicación con la importancia de esa aplicación para la empresa es fundamental en la gestión de riesgos cibernéticos. Esta herramienta no sólo permite priorizar recursos y esfuerzos de seguridad en aplicaciones críticas para el negocio que también presentan un alto riesgo de impacto sino que es extremadamente visual; lo que facilita la toma de decisiones informadas, la formulación de estrategias de seguridad efectivas y la comunicación eficiente de los riesgos de seguridad a todas las partes interesadas. Además, contribuye al cumplimiento de regulaciones y estándares de seguridad y agiliza la respuesta a incidentes de seguridad al identificar rápidamente las áreas más vulnerables.

Número de usuarios por aplicación

Figura 38: Dashboard: Número de usuarios por aplicación.

La cantidad de usuarios que interactúan con una aplicación afecta directamente su superficie de ataque potencial. Cuantos más usuarios, mayor es la exposición a posibles amenazas cibernéticas. Registrar esta cantidad permite a los equipos de gestión de riesgos evaluar la magnitud del riesgo y tomar medidas proporcionales para proteger la aplicación. Un registro de usuarios ayuda a supervisar posibles incidentes y a tomar medidas preventivas para abordar las vulnerabilidades antes de que se conviertan en amenazas reales.

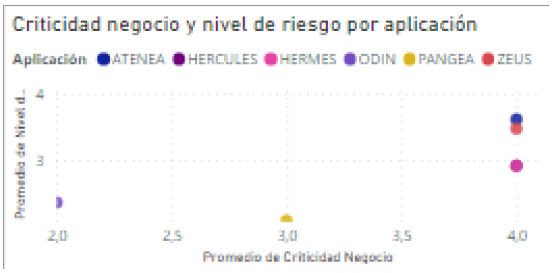
El seguimiento constante de la cantidad de usuarios permite detectar anomalías en el uso de la aplicación. Cambios inesperados en el número de usuarios pueden indicar posibles amenazas, como intentos de acceso no autorizado o ataques. La detección temprana es esencial para tomar medidas preventivas.
Por otro lado, en caso de un incidente de seguridad, como una brecha de datos, conocer la cantidad de usuarios afectados es crucial para evaluar el impacto real del incidente. Esto guía la respuesta de emergencia, la notificación a las partes afectadas y la mitigación de las consecuencias.

Aplicaciones con datos bancarios

Figura 39: Dashboard: Aplicaciones con datos bancarios.

Es importante tener un control riguroso sobre las aplicaciones que manejan datos bancarios por varias razones. En primer lugar, los datos bancarios son altamente sensibles y valiosos, lo que los convierte en objetivos atractivos para atacantes. Una brecha de seguridad en una aplicación que maneja datos bancarios puede tener graves consecuencias financieras y legales, incluyendo pérdida de confianza de los clientes y multas reguladoras. En este caso, el 75 % de las aplicaciones usan datos bancarios, por lo que destaca la importancia de un control riguroso y medidas de seguridad adecuadas para proteger estos datos y garantizar el cumplimiento normativo.

(a) Porcentaje de aplicaciones que usan datos bancarios.



(b) Criticidad de aplicaciones que usan datos bancarios.

(c) Media de CV de aplicaciones que usan datos bancarios.

Figura 40: *Dashboard* para aplicaciones con datos bancarios.

En particular, las aplicaciones Atenea, Zeus, Hércules, Hermes, Odin y Pangea son cruciales para el negocio (Ver 40b), y todas ellas utilizan datos bancarios (Ver 40a). Esta información es vital para priorizar la seguridad de estas aplicaciones, ya que cualquier amenaza o vulnerabilidad en ellas podría tener un impacto significativo en la continuidad de las operaciones y en la confidencialidad de los datos financieros. Además, el hecho de poder rastrear la media de CVSS que afecta a las CVE de cada aplicación (Ver 40c) proporciona una métrica cuantitativa para evaluar la gravedad de las vulnerabilidades específicas que podrían afectar a estas aplicaciones críticas. Esto facilita la asignación de recursos y esfuerzos de seguridad de manera efectiva, centrándose en la mitigación de las amenazas más significativas y en la protección de los activos financieros y la reputación de la empresa.

Servidores

Las aplicaciones suelen ejecutarse sobre servidores, por lo tanto, un listado de servidores proporciona una visión completa de los activos de hardware en la organización. Esto es fundamental para una gestión eficiente de activos, ya que permite realizar un seguimiento de la

ubicación, el estado y la propiedad de los servidores. Además, La información sobre el sistema operativo de cada servidor es esencial para mantener un inventario preciso de software. Dado que las vulnerabilidades pueden estar relacionadas con el sistema operativo, conocer las versiones y configuraciones específicas es crucial para evaluar el riesgo.

Name	IP Address	Operating System	Suma de Media CVEs
Server_1	10.0.102.101	Windows Server 2016	8,80
Server_10	192.168.3.15	Windows Server 2019	5,30
Server_11	192.168.3.188	Windows Server 2022	3,20
Server_12	192.168.3.19	Windows Server 2022	3,20
Server_14	192.168.3.38	Windows Server 2022	3,20
Server_15	192.168.3.40	Windows Server 2022	3,20
Server_16	192.168.3.54	Windows Server 2016	8,80
Server_17	192.168.3.80	Windows Server 2022	3,20
Server_18	192.168.3.90	Windows Server 2022	3,20
Server_19	192.168.3.97	Windows Server 2016	8,80
Server_2	10.254.27.1	Windows Server 2016	8,80

Figura 41: Dashboard: Servidores.

Calcular la suma de la media de CVE en los servidores proporciona una métrica que indica la exposición a vulnerabilidades de la infraestructura. Esto ayuda a priorizar la aplicación de parches y la mitigación de riesgos en los servidores más críticos y vulnerables.

Asimismo, tener un listado de servidores y su configuración es fundamental para la planificación estratégica de la seguridad. Permite identificar áreas donde se necesitan medidas de seguridad adicionales, como firewalls, sistemas de detección de intrusiones o medidas de autenticación más sólidas.

Además de la información proporcionada en la figura 41 sobre los servidores, en el anexo IV se encuentra disponible una tabla detallada que contiene más datos que se han considerado sobre los servidores para una referencia más completa.

En la página de activos se proporciona información detallada sobre los activos utilizados por la organización.

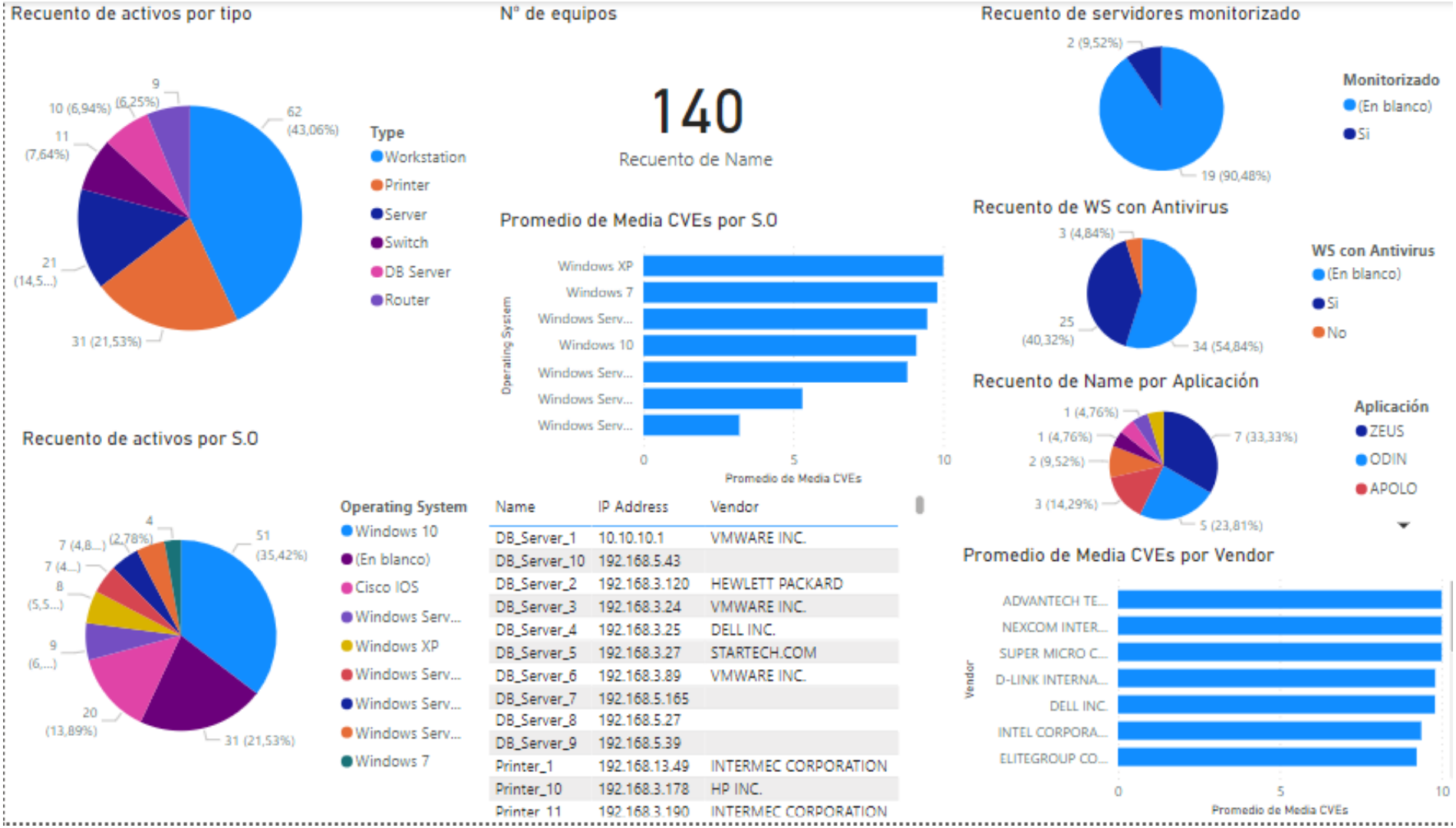


Figura 42: Dashboard activos.

Recuento de activos

Figura 43: Dashboard: Recuento de activos.

La cantidad de activos influye en la priorización de riesgos. Los activos más numerosos pueden tener un impacto significativo en la empresa si se ven comprometidos, por lo que es esencial considerar su cantidad al evaluar los riesgos.

Tipos de activos

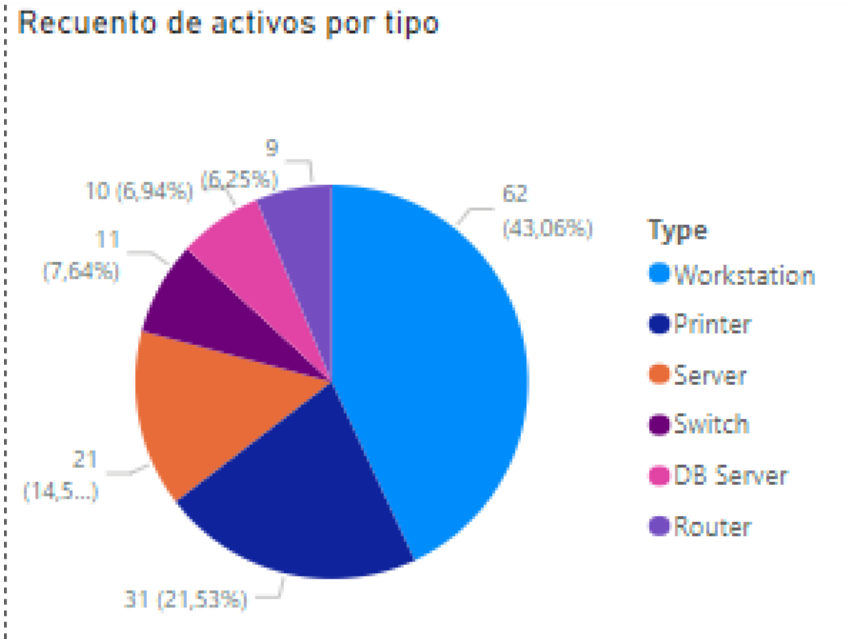


Figura 44: Dashboard: Tipos de activos.

Cada tipo de activo tiene sus propias vulnerabilidades y amenazas específicas. Al tener un recuento de los tipos de activos, la empresa puede identificar los riesgos que son más relevantes para cada categoría y tomar medidas de seguridad adecuadas. Cada tipo de activo puede requerir políticas de seguridad específicas. Por ejemplo, las bases de datos pueden requerir cifrado de datos y autenticación rigurosa, mientras que los dispositivos de red pueden requerir configuraciones de firewall específicas. El conocimiento de los tipos de activos facilita la creación de políticas de seguridad adecuadas.

Además, la pérdida o la compromisión de ciertos tipos de activos pueden tener un impacto significativo en la organización. Por ejemplo, la pérdida de datos de una base de datos crítica puede ser más grave que la pérdida de una impresora. Entender los tipos de activos ayuda a evaluar mejor el impacto potencial de un incidente.

En general, un recuento detallado de los tipos de activos ayuda en la gestión de inventarios, lo que facilita la administración de activos, la planificación de actualizaciones y el mantenimiento adecuado.

S.O de los activos

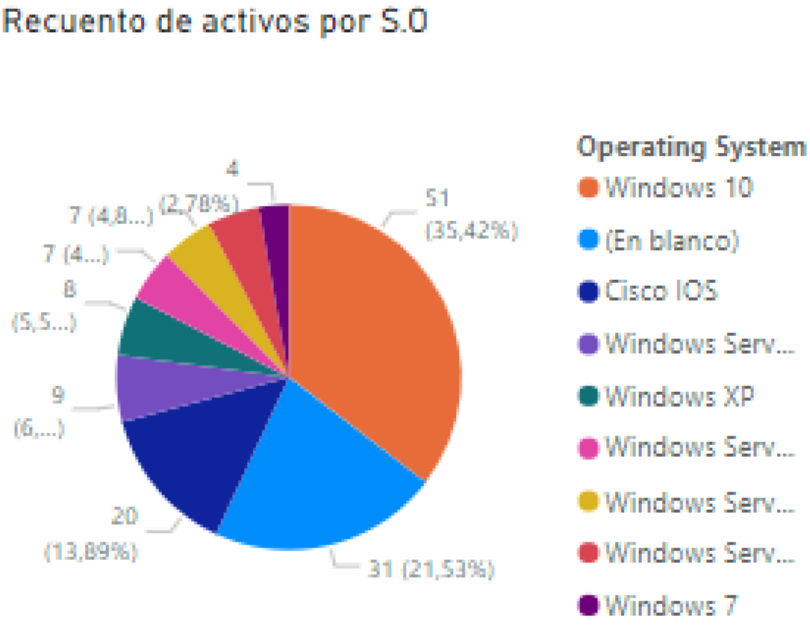


Figura 45: Dashboard: S.O de los activos.

Como se ha comentado antes, cada sistema operativo tiene sus propias vulnerabilidades y amenazas específicas. Al conocer los tipos de SO utilizados en los activos, la organización puede identificar y evaluar los riesgos que afectan a cada plataforma de manera más precisa. Esto permite tomar medidas de seguridad adaptadas a las características de cada SO. Ademñas, los fabricantes de sistemas operativos emiten actualizaciones y parches de seguridad para abordar las vulnerabilidades conocidas. Con un recuento de los tipos de SO, la organización puede priorizar las actualizaciones en función de la importancia de los sistemas operativos y su vulnerabilidad relativa.

Al saber los tipos de SO, se puede evaluar el riesgo potencial de explotación de vulnerabilidades en función de la popularidad y la visibilidad de cada plataforma. Los SO más comunes pueden ser objetivos más atractivos para los atacantes.

Media de CVEs por S.O

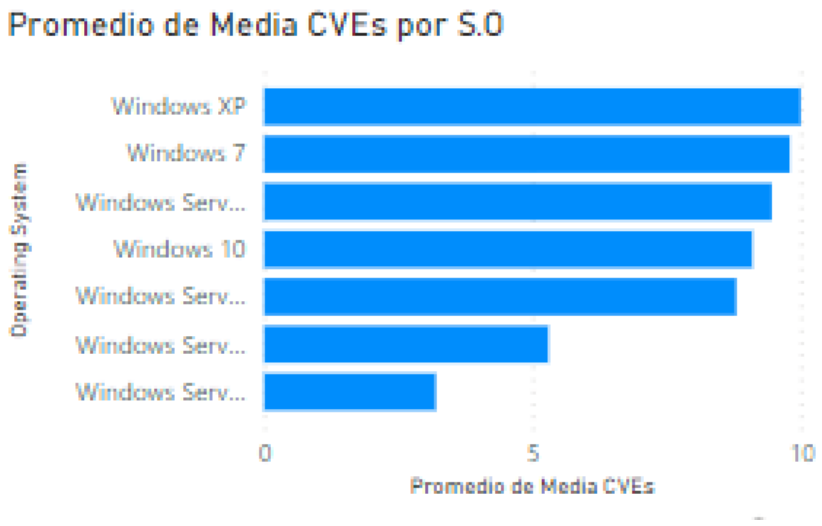


Figura 46: Dashboard: Media de CVEs por S.O.

La media de CVEs por SO proporciona una visión general de la cantidad promedio de vulnerabilidades conocidas que afectan a cada plataforma. Esto ayuda a las organizaciones a identificar qué sistemas operativos pueden ser más propensos a riesgos de seguridad debido a la cantidad de vulnerabilidades asociadas. Cuando se conoce la media de CVEs por SO, las organizaciones pueden priorizar la aplicación de parches y actualizaciones de seguridad en función de la cantidad de vulnerabilidades. Los SO con una media de CVEs más alta pueden requerir una atención especial y actualizaciones más frecuentes. Permite evaluar los riesgos relativos asociados con diferentes SO en el entorno de una organización. Los SO con una media de CVEs más alta pueden ser considerados de mayor riesgo y, por lo tanto, requerir medidas de seguridad adicionales. Mantener un seguimiento de la media de CVEs por SO permite una monitorización continua de la postura de seguridad de la organización. Si la media aumenta significativamente en un SO específico, puede ser una señal de que se requieren acciones urgentes.

Descripción de activos

Name	IP Address	Vendor
DB_Server_1	10.10.10.1	VMWARE INC.
DB_Server_10	192.168.5.43	
DB_Server_2	192.168.3.120	HEWLETT PACKARD
DB_Server_3	192.168.3.24	VMWARE INC.
DB_Server_4	192.168.3.25	DELL INC.
DB_Server_5	192.168.3.27	STARTECH.COM
DB_Server_6	192.168.3.89	VMWARE INC.
DB_Server_7	192.168.5.165	
DB_Server_8	192.168.5.27	
DB_Server_9	192.168.5.39	
Printer_1	192.168.13.49	INTERMEC CORPORATION
Printer_10	192.168.3.178	HP INC.

Figura 47: Dashboard: Descripción de activos.

En la tabla se detallan los activos de la organización, que incluyen servidores, workstations, impresoras, switches y routers. Cada uno de estos activos se identifica mediante información relevante, como la dirección IP (IP Address) y el fabricante o proveedor (Vendor).

La información sobre el fabricante o proveedor (Vendor) es especialmente importante ya que algunas vulnerabilidades de seguridad pueden estar asociadas a fabricantes o proveedores específicos. Esto significa que ciertos dispositivos de un proveedor pueden ser más propensos a ciertos tipos de amenazas . Conocer el proveedor ayuda a identificar estas posibles vulnerabilidades.

Media de CVE por vendor

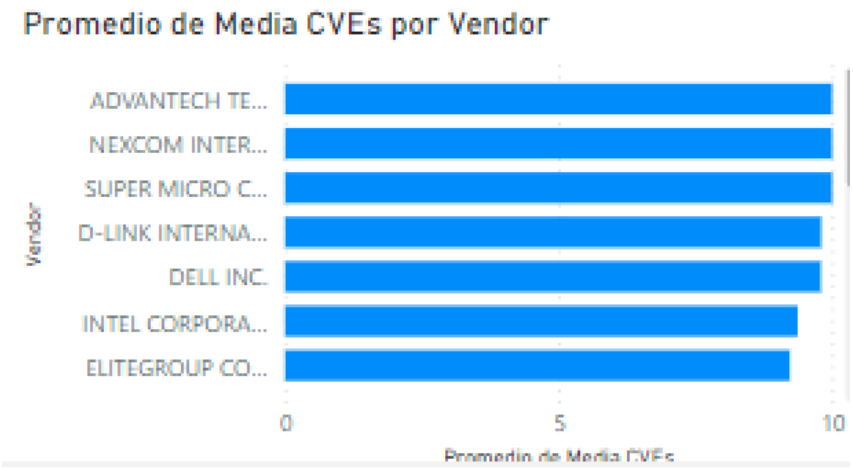


Figura 48: Dashboard: Media de CVE por vendor.

Esta gráfica muestra la media de CVEs por proveedor y permite identificar tendencias en cuanto a la seguridad de los productos de diferentes fabricantes. Si un proveedor en particular tiene consistentemente una media de CVEs más alta que otros, esto puede indicar un problema de seguridad sistémico en sus productos. Además, permite evaluar los riesgos relativos asociados con diferentes proveedores. Si un proveedor tiene una media de CVEs significativamente más alta que otros, sus productos pueden considerarse de mayor riesgo y requerir medidas de seguridad adicionales.

Servidores monitorizados

Figura 49: Dashboard: Servidores monitorizados.

Los servidores que no están siendo monitoreados representan puntos ciegos en la seguridad cibernética de la organización. Esto significa que cualquier actividad maliciosa o anomalía que ocurra en esos servidores podría pasar desapercibida. Contarlos ayuda a identificar estos puntos ciegos y tomar medidas para reducirlos. Es por esto mismo por lo que es importante tener un recuento de los servidores que sí se monitorean y los que no.

WS con antivirus

Los programas antivirus desempeñan un papel fundamental en la detección y prevención de malware y otras amenazas cibernéticas. Contar las estaciones de trabajo con antivirus ayuda a asegurarse de que se esté brindando una capa básica de protección contra amenazas comunes. Las estaciones de trabajo sin antivirus o con antivirus desactualizados pueden ser más vulnerables a ataques cibernéticos.

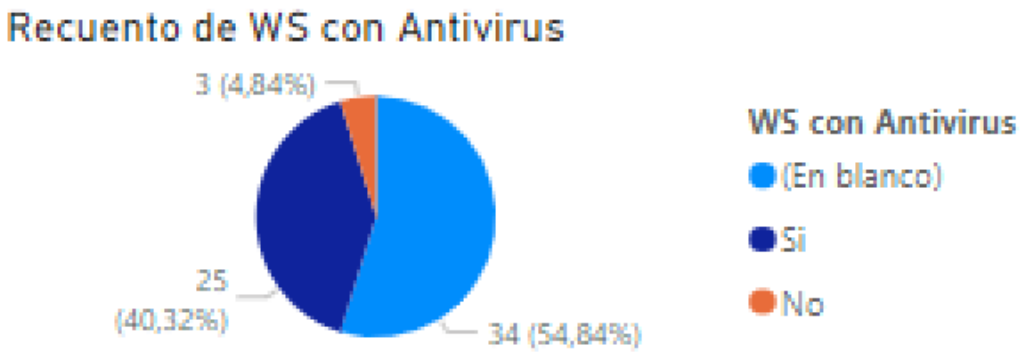


Figura 50: Dashboard: WS con antivirus.

5. Resultados

En este documento se ha demostrado que se ha podido obtener un inventario de activos unificado y centralizado,tal como se aprecia en el dashboard de la metodología. Para ilustrar la importancia de esta consolidación de activos, se consideran dos casos de uso reales. El 11 de julio de 2023, surgió una nueva vulnerabilidad, CVE-2023-32056 [7], y comprender su impacto en la empresa es de vital importancia. Por otro lado es bastante común que las filtraciones de datos bancarios sean un motivo de preocupación importante en el ámbito de la ciberseguridad. Cuando se produce una filtración de datos bancarios, es fundamental determinar a qué aplicaciones y sistemas ha afectado para poder tomar medidas correctivas y mitigar el riesgo de forma efectiva. En estas situaciones, contar con un inventario completo y centralizado de activos es esencial para evaluar de manera rápida y eficaz cuáles de ellos están en riesgo y tomar medidas preventivas de manera. Esto demuestra cómo la gestión de activos de ciberseguridad proporciona la capacidad de respuesta necesaria en momentos críticos para proteger la empresa contra amenazas emergentes.

5.1. Caso de uso I

La CVE-2023-32056 es una vulnerabilidad de seguridad denominada "Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability". Esta vulnerabilidad afecta a sistemas operativos como Windows 10, Windows Server 2019, Windows Server 2022 y Windows 11. Su fecha de publicación fue el 11 de julio de 2023 y se actualizó por última vez el 8 de agosto de 2023.

El impacto de la CVE-2023-32056 en los sistemas operativos mencionados es de suma importancia y requiere una acción inmediata. Para evaluar y abordar esta vulnerabilidad, se realiza un análisis exhaustivo y un filtrado en el dashboard, donde se puede identificar que de los 140 activos de la infraestructura, 65 se han visto afectados por esta vulnerabilidad en particular.
Esto implica que más del 46 % de los activos están en riesgo de explotación a través de esta vulnerabilidad. Como resultado, es crucial tomar medidas inmediatas para mitigar estos riesgos y proteger nuestros activos.

Además, al profundizar en el análisis, se observa que esta vulnerabilidad también afecta a algunas de las aplicaciones. De las 8 aplicaciones de la muestra, 7 de ellas muestran vulnerabilidades relacionadas con esta CVE. De estas, 2 de ellas son consideradas cruciales para el funcionamiento y la continuidad del negocio.
Esto significa que no sólo los sistemas operativos están en riesgo, sino que aplicaciones esenciales para el negocio también podrían verse comprometidas, lo que podría tener un impacto significativo en la operación de la empresa y en la seguridad de los datos.

Dado este panorama, es esencial tomar medidas inmediatas para abordar esta vulnerabilidad. Esto puede incluir la aplicación de parches de seguridad, actualizaciones de software, o cualquier otra acción recomendada por los proveedores de software y las autoridades de ciberseguridad. Además, se debe llevar a cabo una monitorización constante de los activos afectados y las aplicaciones críticas para garantizar que estén protegidos contra posibles amenazas cibernéticas. La rápida respuesta y la priorización de estas medidas son esenciales para mantener la integridad y la seguridad de la infraestructura y datos críticos.

[7] Más información en: https://www.cvedetails.com/cve/CVE-2023-32056/

El impacto de la CVE-2023-32056 en la infraestructura y aplicaciones críticas se ha podido analizar minuciosamente gracias a la sólida base que representa nuestro inventario de activos y su valoración. Este análisis detallado ha sido posible debido a que se cuenta con un registro completo y actualizado de todos los activos, lo que nos ha permitido filtrar y segmentar la información.

Gracias a este inventariado de activos, se ha podido identificar con precisión cuántos y cuáles de los activos se han visto afectados por esta vulnerabilidad. Este conocimiento es fundamental para tomar decisiones informadas y priorizar las acciones de mitigación de riesgos de manera eficiente.

Además, al contar con una valoración de activos que incluye la criticidad de las aplicaciones, se pudo comprender plenamente el alcance de la amenaza. Esto permitió no solo identificar las aplicaciones que se ven afectadas, sino también determinar cuáles de ellas tienen un impacto crítico en nuestro negocio.

Ver figura 51

5.2. Caso de uso II

Las filtraciones de datos bancarios son uno de los tipos de incidentes de seguridad más delicados y críticos que una organización puede enfrentar. Cuando se produce una filtración de este tipo, el impacto potencial es significativo, ya que involucra la exposición de información financiera altamente confidencial.

Conocer las aplicaciones específicas afectadas permite comprender la magnitud del problema. Esto puede ayudar a determinar cuántos registros o datos sensibles se vieron comprometidos y la escala del incidente. En este caso las aplicaciones que se han vist afectadas son: ATENEA, ODIN, ZEUS, HÉRCULES, HERMES, PANGEA, APOLO, HADES.

Como no todas las aplicaciones tienen el mismo nivel de importancia o riesgo asociado, al identificar las aplicaciones afectadas, es posible priorizar la respuesta y enfocar los recursos en las áreas críticas para minimizar el impacto. En este caso, vemos que tanto ZEUS como ATENEA se han visto afectados, y estas aplicaciones son críticas para la empresa.

Una vez identificadas las aplicaciones afectadas, es posible realizar una evaluación más detallada de las vulnerabilidades que condujeron a la filtración de datos. Esto es esencial para corregir las debilidades y prevenir futuros incidentes.

Ver figura 52

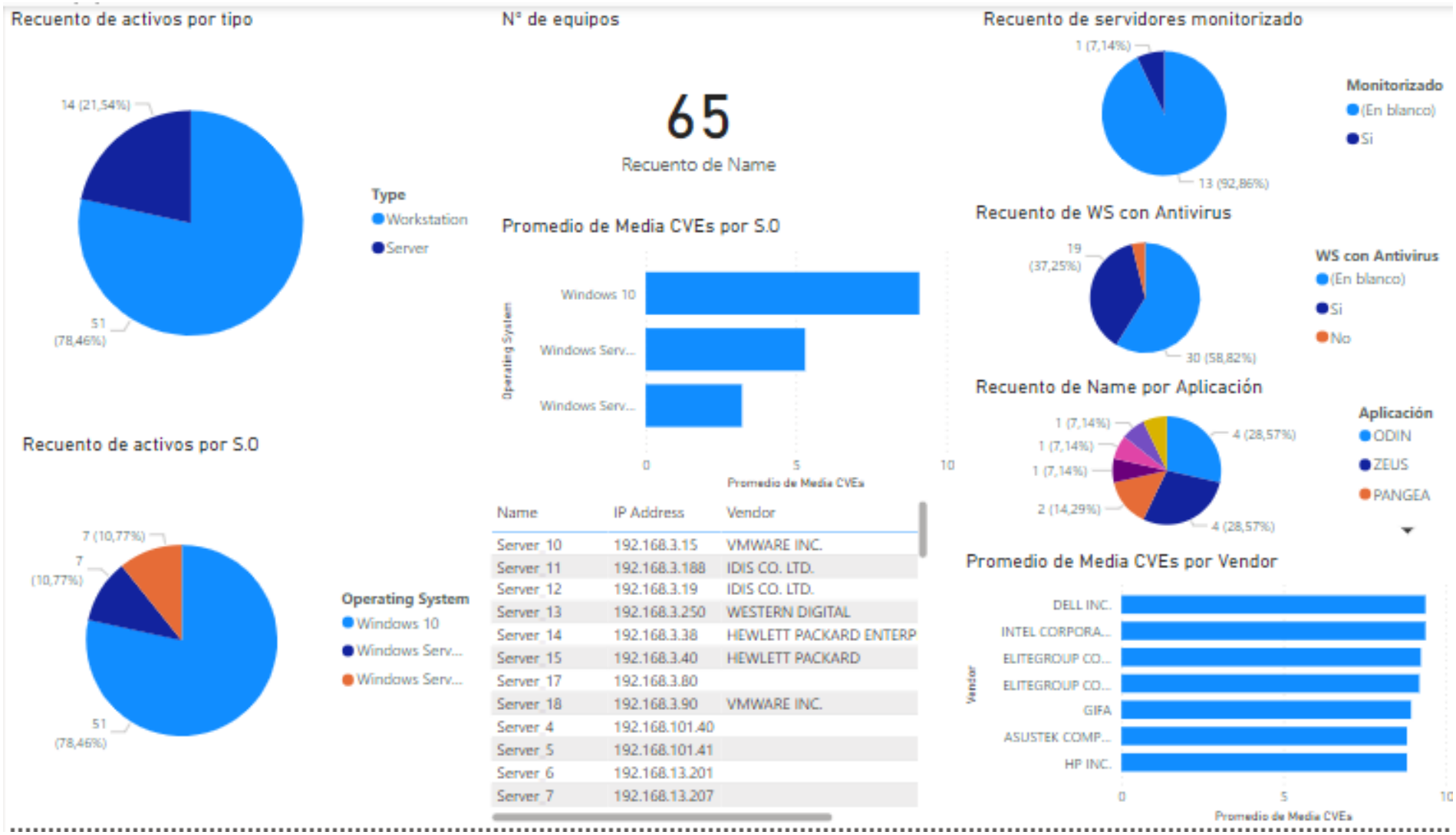
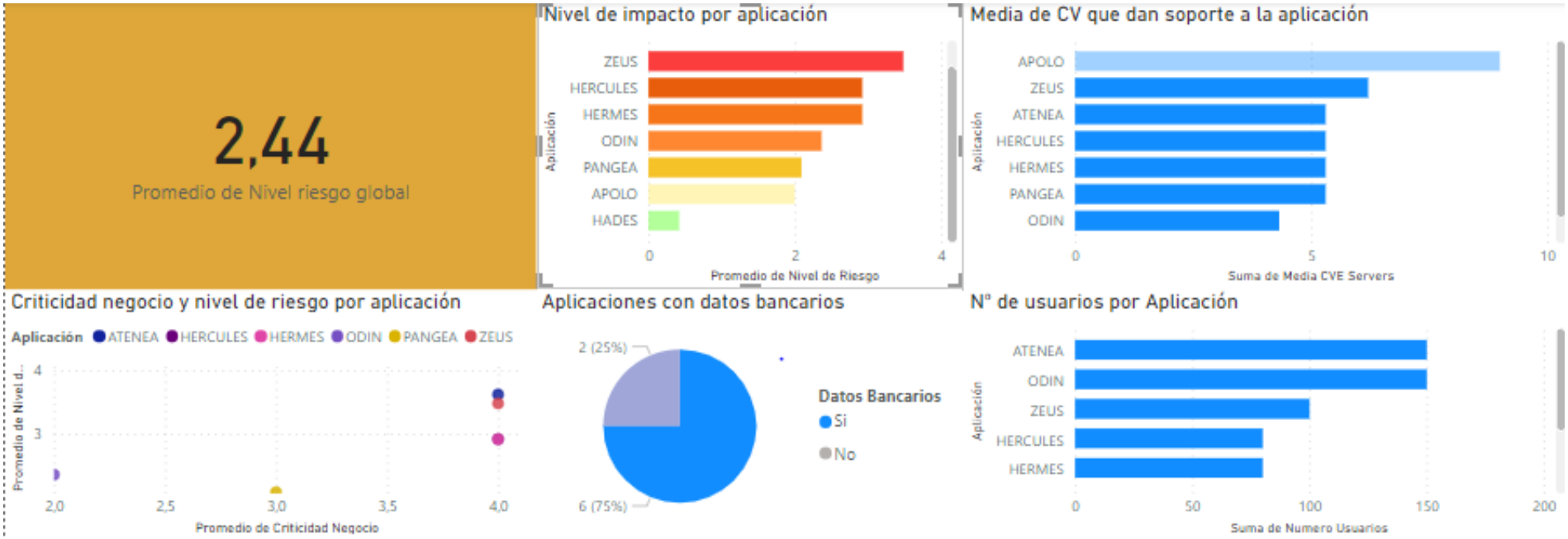


Figura 51: Dashboard caso de uso 1.



Aplicación	Descripción	Tipo de Tecnologia	Media CVE Servers	Suma de Nivel de Riesgo
ATENEA	El sistema integral de gestión de recursos humanos esencial que simplifica la administración de personal y la nómina.	Web	5,30	3
ZEUS	El sistema ERP (Enterprise Resource Planning) esencial de la empresa que centraliza la gestión de recursos empresariales, incluyendo finanzas, recursos humanos, inventario y más, facilitando la coordinación y automatización de las operaciones	Thick-Client	6,20	3
HERCULES	El sistema CRM (Customer Relationship Management) esencial que permite la administración de relaciones con clientes, seguimiento de ventas, marketing y servicio al cliente, mejorando la satisfacción y lealtad de los clientes.	Thick-Client	5,30	2

Name	IP Address	Operating System	Suma de Media CVEs
Server_1	10.0.102.101	Windows Server 2016	8,80
Server_10	192.168.3.15	Windows Server 2019	5,30
Server_11	192.168.3.188	Windows Server 2022	3,20
Server_12	192.168.3.19	Windows Server 2022	3,20
Server_14	192.168.3.38	Windows Server 2022	3,20
Server_15	192.168.3.40	Windows Server 2022	3,20
Server_16	192.168.3.54	Windows Server 2016	8,80
Server_17	192.168.3.80	Windows Server 2022	3,20
Server_18	192.168.3.90	Windows Server 2022	3,20
Server_19	192.168.3.97	Windows Server 2016	8,80
Server_2	10.254.27.1	Windows Server 2016	8,80

Figura 52: Dashboard caso de uso 2.

6. Discusión y Líneas Futuras

En el contexto de esta investigación, se ha priorizado la identificación y valoración de riesgos en el ámbito de la gestión de seguridad de la información. Sin embargo, la gestión de riesgos es un proceso continuo y holístico que abarca múltiples etapas, y existe un amplio campo para futuras investigaciones y desarrollos.

Una de las líneas de investigación que se podría explorar para ampliar y enriquecer este trabajo se refiere a la planificación de estrategias de mitigación. Una vez que los riesgos han sido identificados y valorados, la planificación de estrategias efectivas para reducir, transferir o aceptar estos riesgos se convierte en un paso crítico. Esta fase implica la elaboración de planes detallados que incluyan la implementación de medidas de seguridad específicas, políticas y procedimientos.
Otra área de investigación relevante sería la implementación de controles de seguridad. Una vez que se han definido las estrategias de mitigación, es fundamental llevar a cabo la implementación efectiva de controles de seguridad. Esto puede incluir la adopción de tecnologías de seguridad avanzadas, la capacitación del personal en cuestiones de seguridad y la configuración de políticas de seguridad coherentes en toda la organización.
El monitoreo continuo es otra línea de investigación importante. Dado que la gestión de riesgos es un proceso en constante evolución, establecer un sistema de monitoreo continuo para evaluar la efectividad de las estrategias de mitigación y los controles de seguridad es esencial. Esto implica la recopilación y análisis de datos relevantes para identificar nuevas amenazas o cambios en los riesgos existentes.
Finalmente, la revisión periódica del proceso de gestión de riesgos es una práctica esencial. A intervalos regulares, se debe realizar una evaluación exhaustiva de todas las etapas del proceso. Esto incluye la revisión de la efectividad de las estrategias de mitigación, la identificación de nuevas vulnerabilidades y la adaptación a los cambios en el entorno de seguridad cibernética.

Explorar estas etapas adicionales de la gestión de riesgos no solo proporcionaría una comprensión más completa de la seguridad de la información en una organización, sino que también contribuiría significativamente a fortalecer la postura de seguridad cibernética de la misma. Además, permitiría afrontar los desafíos cibernéticos en constante evolución de manera más efectiva y garantizaría la continuidad de las operaciones de manera segura y resiliente.

7. Conclusiones

La gestión de riesgos es un componente esencial de la ciberseguridad que, durante muchos años, ha estado en la sombra sin la visibilidad que merece. Sin embargo, en los últimos años, ha experimentado un crecimiento significativo en su importancia, y esta tendencia va en aumento. Esta evolución se debe en gran medida a la creciente interconexión y digitalización de sistemas en las organizaciones, lo que ha expuesto a la información y a los activos a nuevas vulnerabilidades y amenazas. Es una disciplina crítica que desafía la percepción tradicional de que la seguridad es simplemente un asunto de implementar medidas de protección. Es un campo en constante evolución que se enfoca en identificar, evaluar, mitigar y supervisar amenazas que pueden afectar a una organización. Su propósito principal es proteger activos críticos, como datos, sistemas y redes, garantizando la continuidad operativa en un entorno cada vez más complejo y peligroso.

En este proyecto, he experimentado tanto desafíos como éxitos. La parte más difícil ha sido unificar, cruzar y centralizar los activos, esto es común en muchos proyectos de gestión de riesgos, ya que la falta de consistencia y estandarización en los datos puede dificultar la identificación precisa de activos y riesgos. Sin embargo, a pesar de estas dificultades, se ha logrado la creación de un inventario de activos unificado y centralizado. Esto es de vital importancia, ya que proporciona una visión completa de los recursos de tecnología de la información de la organización, lo que permite una gestión de la seguridad más eficaz.

Uno de los desafíos adicionales en la gestión de riesgos en ciberseguridad es que existen múltiples estándares y metodologías, cada uno con sus propios pasos y enfoques. Si bien todos comparten el objetivo fundamental de proteger los activos y la información de una organización, la variedad de estándares puede generar confusión. Además, la lectura de estos estándares puede ser una tarea desafiante debido a su lenguaje técnico y su densidad de información. Los estándares suelen ser documentos detallados que requieren tiempo y esfuerzo para comprender completamente. A medida que se avanzaba en la comprensión y aplicación de los conceptos de gestión de riesgos en ciberseguridad, he encontrado una mayor familiaridad con los estándares y sus requisitos. La experiencia y la práctica me han ayudado a superar las dificultades iniciales y a sentirte más cómoda con los conceptos y estándares.

La parte más sencilla del proyecto ha sido el uso de Power BI. Esta herramienta se ha destacado por su intuitiva interfaz y su capacidad para generar resultados esperados. Ha demostrado ser una plataforma eficaz para la visualización de datos, la integración de fuentes diversas y el análisis en tiempo real. Como se ha visto en los casos de uso, Power BI ha permitido gestionar eficientemente situaciones que pueden surgir en la rutina diaria de la empresa, brindando una visión completa y actualizada de los riesgos y facilitando la toma de decisiones informadas.

8. Bibliografía

Referencias

[nis,] Nist releases version 1.1 of its popular cybersecurity framework. https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework. Accedido el 30 Agosto 2023.

[RAE,] Seguro. Real Academia Española (RAE). Exento o libre de peligro, daño o riesgo.

[iso, 2011] (2011). ISO 27005:2011 Information technology - Security techniques - Information security risk management. `http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56742`. Accessed: [26 Agosto 2023].

[ISA, 2021] (2021). ISACA Glossary. ISACA.

[isa, 2021] (2021). *Manual de preparación para el examen CISM*. 15ª edition.

[Agence nationale de la sécurité des systémes d'information (ANSSI),] Agence nationale de la sécurité des systémes d'information (ANSSI). Ebios risk manager: Going further. https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios$_r isk_m anager - going_f urther - en - v$1,0.*pdf*. *Accedidoel*31*Agosto*2023.

[Agence nationale de la sécurité des systèmes d'information (ANSSI),] Agence nationale de la sécurité des systèmes d'information (ANSSI). Ebios risk manager – the method. `https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/`.

[Arimetrics, 2023] Arimetrics (2023). Glosario power bi.

[Asana, 2023] Asana (Último acceso: 9 Septiembre 2023). Top-down approach in project management. Accedido el 7 Agosto 2023.

[Briceño, 2021] Briceño, E. V. (2021). *Seguridad de la información*. 3Ciencias.

[Centro Criptológico Nacional, 2022] Centro Criptológico Nacional (2022). APROXIMACIÓN AL MARCO DE GOBERNANZA DE LA CIBERSEGURIDAD.

[de Gobierno Electrónico y Sociedad de la Información y del Conocimiento., 2021] de Gobierno Electrónico y Sociedad de la Información y del Conocimiento., A. (2021). Estudio comparado de metodologías de análisis de riesgos para ti y seguridad de la información. `https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/book/6611/download`.

[García, 2019] García, L. J. (2019). Gestión de la ciberseguridad.

[Gashgari et al., 2017] Gashgari, G., Walters, R. J., and Wills, G. B. (2017). A proposed best-practice framework for information security governance. In *IoTBDS*, pages 295–301.

[IBM,] IBM. ¿qué es el marco de ciberseguridad del nist? https://www.ibm.com/es-es/topics/nist. Accedido el 30 Agosto 2023.

[INCIBE-CERT, 2023] INCIBE-CERT (2023). Cvss 3.0.

[Instituto Nacional de Ciberseguridad, 2016] Instituto Nacional de Ciberseguridad (2016). *Gestión de riesgos: Una guía de aproximación para el empresario.*

[International Organization for Standardization, 2013] International Organization for Standardization (2013). ISO 27001 - Information technology - Security techniques - Information security management systems - Requirements.

[ISACA, 2018a] ISACA (2018a). Information security architecture gap assessment and prioritization. *ISACA Journal*, Volumen 2.

[ISACA, 2018b] ISACA (2018b). Information security architecture gap assessment and prioritization. *ISACA Journal*, Volumen 2.

[Lisa Institute,] Lisa Institute. Diferencia entre ciberseguridad, seguridad informática y seguridad de la información.

[Martínez, 2018] Martínez, R. B. (2018). Gobierno de la ciberseguridad. *Economía industrial*, (410):61–70.

[Mengual Galán, 2005] Mengual Galán, L. (2005). Arquitecturas de seguridad. *Recuperado de: http://www. personal. fi. upm. es/˜ lmengual/ARQ_REDES/Arquitecturas_Seguridad. pdf.*

[Microsoft, ceso] Microsoft (Año de acceso). Power bi overview.

[Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), 2016] Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) (2016). Guía de gestión de riesgos. seguridad y privacidad de información - guía no. 7. `https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf`.

[MITRE Corporation, 1999] MITRE Corporation (1999). CVE (Common Vulnerabilities and Exposures). ciberseguridad.com.

[of France, 2023] of France, N. C. A. (2023). *MAPPING THE INFORMATION SYSTEM How-to guide in 5 steps.* National Cybersecurity Agency of France.

[Ordr, 2023] Ordr (2023). The increasing importance of cybersecurity asset management. `https://ordr.net/article/increasing-importance-of-cybersecurity-asset-management/`.

[Organización Internacional de Normalización, 2013] Organización Internacional de Normalización (2013). ISO 27001 : Information technology. Security techniques. Information security management systems, requirements.

[Red Hat,] Red Hat. What is CVE? Consultado el 1 Septiembre 2023.

[WebLinus, 2023] WebLinus (2023). Cuota de mercado de los sistemas operativos actuales.

9. Anexos

Anexo I

EJEMPLOS DE VULNERABILIDADES Y AMENAZAS (ISO 27005)

TIPO	EJEMPLO DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
Hardware	Mantenimiento insuficiente / instalación fallida de medios de almacenamiento	Brechas de mantenimiento del sistema de información
	Falta de esquemas de reemplazo periódico	Destrucción de equipamiento o medios
	Susceptible a humedad, polvo	Polvo, corrosión
	Sensibilidad a radiación electromagnética	Radiación electromagnética
	Falta de un eficiente control de cambios en la configuración	Error en el uso
	Susceptible a variaciones de voltaje	Pérdida de alimentación eléctrica
	Susceptible a variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento desprotegido	Robo de medios o documentos
	Falta de cuidado en el desecho / disposición de equipos	Robo de medios o documentos
	Falta de control de copiado	Robo de medios o documentos
Software	Falta o insuficiencia de pruebas de software	Abuso de privilegios
	Fallas conocidas en el software	Abuso de privilegios
	Falta de controles para el cierre de sesión en terminales desatendidas	Abuso de privilegios
	Desecho o reutilización de medios de almacenamiento sin un borrado apropiado	Abuso de privilegios
	Falta de pistas de auditoría	Abuso de privilegios
	Incorrecta asignación de privilegios de acceso	Abuso de privilegios
	Software ampliamente distribuido	Corrupción de datos
	Aplicación de programas de aplicación a datos erróneos en términos de tiempo	Corrupción de datos
	Interfaz de usuario complicada	Error en el uso
	Falta de documentación	Error en el uso
	Parametrización incorrecta	Error en el uso
	Fechas incorrectas	Error en el uso
	Falta de mecanismos de identificación y autenticación	Suplantación de identidad
	Tablas de claves secretas (passwords) desprotegidos	Suplantación de identidad
	Pobre gestión de claves secretas (passwords)	Suplantación de identidad
	Servicios innecesarios habilitados	Procesamiento ilegal de datos
	Software inmaduro	Malfuncionamiento de software
	Especificaciones poco claras o incompletas para desarrolladores	Malfuncionamiento de software
	Falta de un control de cambios efectivo	Malfuncionamiento de software
	Descarga y uso de software no controlados	Manipulación de software
	Falta de copias de respaldo	Manipulación de software
	Falta de protección física del edificio, puertas y ventanas	Robo de medios o documentos
	Falta de control para la producción de reportes gerenciales	Uso no autorizado de equipamiento

TIPO	EJEMPLO DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
Red	Falta de prueba del envió o recepción de un mensaje	Denegación de acciones
	Líneas de comunicación desprotegidas	Espionaje
	Tráfico sensible desprotegido	Espionaje
	Cableado unido pobremente	Falla de equipos de telecomunicación
	Punto único de falla	Falla de equipos de telecomunicación
	Falta de identificación y autenticación de emisor y receptor	Suplantación de identidad
	Arquitectura de red insegura	Espionaje remoto
	Transferencia de claves secretas en texto plano	Espionaje remoto
	Inadecuada gestión de riesgos	Saturación de sistemas de información
	Conexiones a redes públicas desprotegidas	Uso no autorizado de equipo
Personal	Ausencia de personal	Brechas en la disponibilidad del personal
	Procedimientos inadecuados de reclutamiento	Destrucción de equipo o medios
	Entrenamiento de seguridad insuficiente	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de concientización en seguridad	Error en el uso
	Falta de mecanismos de monitoreo	Procesamiento ilegal de datos
	Trabajo del personal de limpieza no supervisado	Robo de medios o documentos
	Falta de políticas para el uso correcto de medios de telecomunicación y mensajería	Uso no autorizado de equipo
Centro de cómputo	Uso inadecuado o descuidado de controles de acceso físico a edificios y cuartos	Destrucción de equipo o medios
	Localización en un área susceptible a inundaciones	Inundación
	Alimentación de energía eléctrica inestable	Pérdida de provisión de energía eléctrica
	Falta de protección física del edificio, puertas y ventanas	Robo de equipo
Organización	Falta de procedimientos formales para el registro y des-registro de usuarios	Abuso de privilegios
	Falta de procedimientos formales para la revisión de derechos de acceso (supervisión)	Abuso de privilegios
	Falta o insuficiencia de provisiones (relativas a seguridad) en contratos con clientes y/o terceras partes	Abuso de privilegios
	Falta de procedimientos para el monitoreo de instalaciones de procesamiento de información	Abuso de privilegios
	Falta de auditorías regulares (supervisión)	Abuso de privilegios
	Falta de procedimientos para la identificación y evaluación de riesgos	Abuso de privilegios
	Falta de reportes de falla registrados en bitácoras de administrador y operador	Abuso de privilegios
	Mantenimiento de servicios inadecuado	Brechas en el mantenimiento de sistemas de información
	Falta o insuficiencia de acuerdos de niveles de	Brechas en el mantenimiento de

TIPO	EJEMPLO DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
	servicio	sistemas de información
	Falta de procedimientos de control de cambios	Brechas en el mantenimiento de sistemas de información
	Falta de procedimientos formales para el control de documentos del Sistema de Gestión de Seguridad de la Información	Corrupción de datos
	Falta de procedimientos formales para la supervisión de registros del Sistema de Gestión de Seguridad de la Información	Corrupción de datos
	Falta de procesos formales para la autorización de información públicamente disponible	Datos de fuentes no confiables
	Falta de asignación apropiada de responsabilidades de seguridad de la información	Denegación de acciones
	Falta de planes de continuidad	Falla de equipos
	Falta de políticas de uso de correo electrónico	Error en el uso
	Falta de procedimientos para la introducción se software en sistemas operativos	Error en el uso
	Falta de registros en las bitácoras de administrador y operador	Error en el uso
	Falta de procedimientos para el manejo de información clasificada	Error en el uso
	Falta de descripciones de puesto que indiquen responsabilidades de seguridad de la información	Error en el uso
	Falta o insuficiencia de provisiones (respecto a la seguridad de la información) en contratos con empleados	Procesamiento ilegal de datos
	Falta de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Robo de equipo
	Falta de control de activos fuera de las instalaciones	Robo de equipo
	Falta o insuficiencia de políticas de “escritorio limpio” y “pantalla limpia”	Robo de medios o documentos
	Falta de autorización de instalaciones de procesamiento de información	Robo de medios o documentos
	Falta de mecanismos de monitoreo establecidos para violaciones a la seguridad	Robo de medios o documentos
	Falta de revisiones de la gerencia en forma regular	Uso no autorizado de equipo
	Falta de procedimientos para el reporte de debilidades de seguridad	Uso no autorizado de equipo
	Falta de procedimientos de provisiones de cumplimiento con derechos de propiedad intelectual	Uso de software falsificado o copiado

APPENDIX 1
DEFINITION AND SUGGESTION OF CONTENT FOR THE DIFFERENT VIEWS

This appendix **defines the different views presented during Step 1** and suggests content ideas for each one. We recommend **selecting the elements to be listed from among these suggestions**, and **possibly completing them** depending on the organisation's requirements and context. The elements proposed for the different views are not necessarily all meant to be shown in the diagrams.

Each element has its corresponding level of detail. Three ascending levels are listed in this guide:

- **1 - minimum level of detail:** essential information;
- **2 - medium level of detail:** key information;
- **3 - in-depth level of detail:** useful information.

The objects and attributes mentioned in the various tables of this appendix, along with the associated levels of detail, are suggestions that tie in consistently with the timeline proposed in Appendix 2. When defining its mapping target and timeline, each organisation is free to define new objects or attributes and to adapt each element's level of detail as required.

Note

The attributes mentioned in blue are geared towards cybersecurity.

1 Ecosystem view

The ecosystem view describes **all of the entities or systems that gravitate around the information system** for which the mapping is being carried out. This view makes it possible to define the **scope of the mapping** and to obtain an **overview of the ecosystem**, without making do solely with an individual study of each entity.

Object	Attribute	Level of detail	Pivot object
Entity or system	Identification and description	1	
	Type of entity or system (e.g. internal, external, provider, customer)		
	Security level (e.g. maturity, security measures in place or defined contractually, degree of trust, accreditation)		
	List of processes supported		View 2
	Entity's security point of contact (e.g. cybersecurity manager)		
Relationship	Type (e.g. provision of goods, services, sales partnership)	1	
	Contractual or statutory link	2	
	Relationship's level of functional importance		

2 Business view of the information system

The business view of the information system describes **all of the organisation's business processes with the stakeholders involved**, regardless of the technological choices made by the organisation and the resources placed at its disposal. The business view is crucial as it enables **the technical elements to be repositioned in their business environment and thus for their context of use to be understood**.

A process is described from start to finish, from the trigger event right through to the final outcome, regardless of any partitioning existing within the organisation. For cross-cutting processes under the governance of several entities,

a structure must be planned to describe them in their entirety – retaining a perception shared by all of the stakeholders.

This view also displays the organisation's information – some of which may be critical and represent preferred targets during attacks.

Object	Attribute	Level of detail	Pivot object
Macro process	Identification and description	2	
	Incoming and outgoing elements		
	List of constituent processes		
	Security requirements (CIAT)		
	Owner	3	
Process	Identification and description	1	
	Incoming and outgoing elements		
	List of constituent activities (or constituent operations where maturity levels 1 or 2[9] are targeted)		
	List of associated systems of entities		View 1
	List of supporting applications		View 3
	Security requirements (CIAT)		
	Owner		
Activity	Identification and description	3	
	List of constituent operations		
Operation	Identification and description	1	
	List of constituent tasks	3	
	List of stakeholders involved	2	
Task	Identification and description	3	
Stakeholder	Name and contact information	2	
	Type: person, group, entity, etc.		
	Type: internal or external to the organisation		

9 – As defined in Appendix 2.

Object	Attribute	Level of detail	Pivot object
Information	Identification and description	1	
	Owner		
	Administrator		
	Storage (type, location)		
	Associated process		
	Security requirements (CIAT)		
	Sensitivity: personal data, medical data, classified data, etc.		
	Regulatory and standards-related requirements	3	

3 Application view

The application view is an opportunity to describe part of what is traditionally referred to as the IT system. This view describes **the technological solutions supporting the business processes** – primarily the applications.

From a cybersecurity point of view, application flows are considered to be of major importance. This view is particularly useful for viewing information exchanges from a software perspective. The exchange arrangements are characterised here in detail.

Object	Attribute	Level of detail	Pivot object
Application unit	Identification and description	2	
	Manager		
	List of constituent applications		
Application	Identification and description	1	
	List of using entity(ies)	2	View 1
	Entity responsible for operations		
	Cybersecurity manager	1	
	Type of technology: thick-client, Web, etc.		

Object	Attribute	Level of detail	Pivot object
Application	Type of application: internal development, software, software package, script, EAI/ESB platform, etc.	1	
	Volume of users and profiles	2	
	Associated flows	1	
	Security requirements (CIAT)		
	External exposure (e.g. Software as a Service – SaaS type solution)		
	List of processes using the application		View 2
	List of application services delivered by the application	2	
	List of databases used by the application	1	
	List of logical servers supporting the application		View 5
Application service	Identification and description	2	
	List of constituent modules		
	Associated flows		
	External exposure (e.g. Cloud service)		
Module	Identification and description	2	
	Associated flows		
Database	Identification and description	1	
	List of using entity(ies)	2	View 1
	Entity responsible for operations		
	Cybersecurity manager	1	
	Type of technology		
	Associated flows		
	List of information contained		View 1
	Security requirements (CIAT)		
	External exposure		
Flows	Identification and description	1	
	Emitter: application, module, database, etc.		
	Receiver: application, module, database, etc.		
	Encryption		

4 Administration view

The administration view is a special case of the application view. It lists the **privilege levels and scopes of administrators**.

The diagram setting out this view is only of use in the case of centralised management of administration access rights to devices comprising several administration scopes. Where the access rights to devices are managed by local accounts, it is reduced to a list of accounts and associated rights for each device.

Object	Attribute	Level of detail
Zone of administration	Identification and description	1
	Group of administrators and privilege levels	
	List of elements contained in the zone	
	List of secrets associated with the administration of resources	
Administration directory service	Identification and description	1
	Solution: Active Directory, Novell, NT4, Samba, etc.	
Active Directory Forest / LDAP Tree Structure	Identification and description	1
	Domains belonging to the forest/tree structure	
	Inter-forest/inter-tree relationships: domains, two-way, filtered, transitive, etc.	
Active Directory / LDAP Domain	Identification and description	1
	Number of domain controllers	
	Number of user accounts attached	
	Number of machines attached	
	Inter-domain relationships: domains, two-way, filtered, etc.	

5 Logical infrastructure view

This view corresponds to the **logical distribution of the network**. It illustrates **the partitioning of networks and logical links between them**. Moreover, it lists the network devices in charge of traffic.

The logical locations of security devices (sensor, firewall, SIEM, etc.) are also listed in this view.

Object	Attribute	Level of detail	Pivot object
Network	Identification and description	1	
	Type of protocol		
	Operations manager		
	Cybersecurity manager		
	Sub-networks attached		
	Level of sensitivity or classification		
Sub-network	Identification and description	1	
	Address/Mask		
	Gateway		
	IP address range: start and end address		
	IP assignment method: static or dynamic		
	Operations manager		
	DMZ or not		
	List of interconnected sub-networks		
	Possibility of wireless access		
Entry gateway from the outside	Technical characteristics	1	
	Public and private IP address		
	Type of authentication		
Connected external entity	Name, Cybersecurity Manager, IS contacts	2	
	Internal networks interconnected to the entity		

Object	Attribute	Level of detail	Pivot object
Switch	Identification: IP address and identifier	1	
	Technical characteristics: model, embedded software version		
	Network flow filtering rules	2	
	Physical support device (if virtualised)		View 6
Router	Identification: IP address and identifier	1	
	Technical characteristics: model, embedded software version		
	Network flow filtering rules	2	
	Physical support device (if virtualised)		View 6
Security device	Identification (identifier, IP address, MAC address) and description	1	
	Technical characteristics: type of device (sensor, firewall, SIEM, etc.), model, OS and version, embedded software version		
	Physical support device (if virtualised)	2	View 6
DHCP server	Identification (identifier, IP address if static, MAC address) and description	2	
	Technical characteristics: model, OS and version		
	Physical support server (if virtual machine)		View 6
DNS server	Identification (identifier, IP address if static, MAC address) and description	2	
	Technical characteristics: model, OS and version		
	Physical support server (if virtual machine)		View 6
Logical server	Identification (identifier, IP address, MAC address) and description	1	
	Technical characteristics: model, OS and version		
	Active network services		
	Physical support server	2	View 6
	Linked applications	1	View 3

6 Physical infrastructure view

The physical infrastructure view **describes the physical devices** making up or used by the information system. This view corresponds to the **geographic distribution of network devices within the different sites of the organisation**. It provides an overview of the assets connected to the company's telecommunication network.

Object	Attribute	Level of detail	Pivot object
Site	Identification and description	1	
	Buildings attached		
Building/Room	Identification and description	1	
	Bays attached		
Bay	Identification and description	1	
	List of hosted machines		
Physical server	Identification: identifier, IP address, DNS name	1	
	Technical characteristics: type, model, OS and version		
	Physical location: site, building, room, bay		
	Logical server(s) attached		View 5
	List of connected switches		
	Operations Manager		
Workstation	Identification	2	
	Technical characteristics: type (desktops or laptops), model, OS and version		
	Physical location: site, building, room		
Storage infrastructure	Identification	2	
	Technical characteristics: type (NAS, SAN, hard drive, etc.), model		
	Physical location: site, building, room, bay		

Object	Attribute	Level of detail	Pivot object
Peripheral	Identification	2	
	Technical characteristics: type (printer, scanner, etc.), model		
	Operations Manager		
Telephone	Identification	2	
	Technical characteristics: type (desktop or laptop), model		
	Physical location: site, building, room		
Physical switch	Identification	1	
	Logical switch(es) attached		View 5
	Technical characteristics: level (L1, L2, L3, etc.), model, embedded software version		
	Physical location: site, building, room, bay		
	VLAN associated		
Physical router	Identification	1	
	Logical router associated		View 5
	Technical characteristics: model, embedded software version		
	Physical location: site, building, room, bay		
	VLAN associated		
Wi-Fi terminal	Identification	2	
	Technical characteristics: model		
	Physical location: site, building, room, bay		
Physical security device	Identification (identifier, IP address, MAC address) and description	1	
	Logical security device(s) attached		View 5
	Technical characteristics: type of device (sensor, firewall, SIEM, etc.), model, OS and version, embedded software version		
	Physical location: site, building, room		
WAN	Identification	1	
	MAN or LAN attached		

Anexo III

Aplicación	Descripción	Manager	CyberManager	Tipo Tecnología	Tipo Aplicación	Núm. Usuarios	Exposición	Criticidad Negocio	Nivel Riesgo	Media CVE	Datos Bancarios
ZEUS	El sistema ERP (Enterprise Resource Planning) esencial de la empresa que centraliza la gestión de recursos empresariales, incluyendo finanzas, recursos humanos, inventario y más, facilitando la coordinación y automatización de las operaciones	Jonh Doe	Jane Doe	Thick-Client	Internal development	100		4	3.48	6.2	Sí
ODIN	Herramienta de gestión de documentos	Jonh Doe	Jane Doe	Web	Software	150		2	2.36	4.32	Sí
APOLO	La aplicación de análisis de datos crítica que proporciona información estratégica para tomar decisiones empresariales fundamentadas.	Jonh Doe	Jane Doe	Thick-Client	Software	20	SaaS	2	2.00	8.99	No
HERMES	La aplicación de seguimiento y gestión de la cadena de suministro vital para optimizar la logística y las operaciones de entrega.	Jonh Doe	Jane Doe	Thick-Client	Internal development	80		4	2.92	5.3	Sí
HERCULES	El sistema CRM (Customer Relationship Management) esencial que permite la administración de relaciones con clientes, seguimiento de ventas, marketing y servicio al cliente, mejorando la satisfacción y lealtad de los clientes.	Jonh Doe	Jane Doe	Thick-Client	Software	80		4	2.92	5.3	Sí
ATENEA	El sistema integral de gestión de recursos humanos esencial que simplifica la administración de personal y la nómina.	Jonh Doe	Jane Doe	Web	Software	150	SaaS	4	3.62	5.3	Sí
PANGEA	La aplicación de comercio electrónico clave que facilita la creación y administración de tiendas en línea, impulsando las ventas y la presencia en línea.	Jonh Doe	Jane Doe	Web	Software	50		3	2.09	5.3	Sí
HADES	La suite de seguridad informática crítica que protege los activos digitales de la empresa y garantiza la conformidad con las regulaciones de seguridad, evitando amenazas cibernéticas	Jonh Doe	Jane Doe	Thick-Client	Software	10	SaaS	1	0.42	3.2	No

Figura 53: Descripción de aplicaciones y riesgos asociados

Anexo IV

IP Address	Name	Operating System	Tipo IP	Type	Aplicación	Media CVEs	Monitorizado
10.0.102.101	Server_1	Windows Server 2016	Privada	Server	ZEUS	8,8	Si
10.254.27.1	Server_2	Windows Server 2016	Privada	Server	ODIN	8,8	Si
192.168.101.249	Server_3	Windows Server 2016	Privada	Server	APOLO	8,8	Si
192.168.101.40	Server_4	Windows Server 2019	Privada	Server	HERMES	5,3	Si
192.168.101.41	Server_5	Windows Server 2019	Privada	Server	HERCULES	5,3	Si
192.168.13.201	Server_6	Windows Server 2019	Privada	Server	ATENEA	5,3	Si
192.168.13.207	Server_7	Windows Server 2019	Privada	Server	PANGEA	5,3	Si
192.168.13.210	Server_8	Windows Server 2019	Privada	Server	PANGEA	5,3	Si
192.168.3.121	Server_9	Windows Server 2019	Privada	Server	ZEUS	5,3	Si
192.168.3.15	Server_10	Windows Server 2019	Privada	Server	ZEUS	5,3	No
192.168.3.188	Server_11	Windows Server 2022	Privada	Server	ZEUS	3,2	Si
192.168.3.19	Server_12	Windows Server 2022	Privada	Server	ODIN	3,2	No
192.168.3.250	Server_13	Windows Server 2022	Privada	Server	HADES	3,2	No
192.168.3.38	Server_14	Windows Server 2022	Privada	Server	ODIN	3,2	Si
192.168.3.40	Server_15	Windows Server 2022	Privada	Server	ODIN	3,2	Si
192.168.3.54	Server_16	Windows Server 2016	Privada	Server	ZEUS	8,8	Si
192.168.3.80	Server_17	Windows Server 2022	Privada	Server	ODIN	3,2	No
192.168.3.90	Server_18	Windows Server 2022	Privada	Server	ZEUS	3,2	No
192.168.3.97	Server_19	Windows Server 2016	Privada	Server	ZEUS	8,8	No
192.168.5.139	Server_20	Windows Server 2012 R2	Privada	Server	APOLO	9,37	Si
192.168.5.31	Server_21	Windows Server 2016	Privada	Server	APOLO	8,8	No

Figura 54: Descripción de servidores