ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"DISEÑO E IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD DE NIVEL 0 A NIVEL1 BASADO EN LAS NORMAS ISO 27002 :2013"

TRABAJO DE TITULACIÓN

Previa a la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Dalton Gonzalo Hernández García

GUAYAQUIL - ECUADOR

AÑO: 2019

AGRADECIMIENTO

Doy gracias a toda mi familia quienes me alientan desde siempre a cumplir mis metas, por ellos celebro este nuevo logro y les agradezco por impulsarme y animarme ante cualquier dificultad. Por toda su confianza en mí, me es grato poder aprovechar y extender mi más sincero agradecimiento.

A los docentes y tutor que formaron parte de este proyecto y contribuyeron a mi crecimiento y formación académica, compartiendo sus conocimientos y experiencias laborales.

A mis compañeros, que hicieron divertido este proceso de aprendizaje, gracias por su excelente predisposición y apoyo en lo que necesitaba.

DEDICATORIA

A mis padres y hermanos por su constante apoyo en mis metas, para mi futura esposa que me alienta en todo momento y se ha convertido en uno de mis pilares y motivaciones para el cumplimiento de mis objetivos.

TRIBUNAL DE SUSTENTACIÓN

_____

DIRECTOR MSIG / MSIA

ING. LENÍN FREIRE

_____

DIRECTOR DEL PROYECTO DE GRADUACIÓN

ING. FABIÁN BARBOZA

_____

MIEMBRO DEL TRIBUNAL

ING. KARINA ASTUDILLO

DECLARACIÓN EXPRESA

Declaro mediante este escrito de forma expresa que la autoría y la responsabilidad de esta tesis de grado me corresponde de forma exclusiva, por lo que manifiesto mi consentimiento para que la universidad ESPOL publique este trabajo a través de cualquier medio en el tiempo que crea conveniente con el objetivo de promover la investigación.

Dalton Gonzalo Hernández García

RESUMEN

Diseñar e implementar un esquema de seguridad de nivel 0 a nivel 1 basado en normas ISO 27002:2013, dicha norma contiene controles de seguridad de la información actualizados, que son aplicables a cualquier empresa indistintamente de su dimensión y naturaleza. La solución propuesta, así como su implementación brindará un nivel de seguridad personalizado para la organización con la finalidad de proteger sus activos, mantener la estabilidad en los procesos y apoyar al cumplimiento de los objetivos de la compañía.

La información en la actualidad es considerada como uno de los activos más importantes en una organización, por lo que la misma debe cumplir con las siguientes características fundamentales: confidencialidad, integridad, y disponibilidad. Esta información generada por la operación del negocio es vulnerable sin la existencia de controles que permitan resguardar los activos y procesos, por lo que se propone la implementación de un esquema de seguridad de la información.

Las políticas de control que formarán parte del esquema de seguridad tendrán base en la norma ISO 27002 versión del 2013, la cual contiene un total de 114 controles, el criterio de selección de los mismos está basado en la operación de la empresa y la necesidad de disminuir la probabilidad de materialización de una amenaza.

El resultado de la aplicación del esquema de seguridad será medible y escalable de tal forma que permita aplicar afinamientos durante y posterior al despliegue; será medido con el nivel de riesgo antes y después de la implementación. En relación a la escalabilidad, se puede ampliar el alcance aumentando controles para los procesos que forman parte de este estudio o mantener los controles inicialmente propuestos, pero con un mayor nivel de restricción.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Hoy en día la información es uno de los activos más importantes de una organización, en la actualidad es la parte más sensible y vulnerable, esto se basa al número de incidentes que se registran por empresas que sufren de algún tipo de interrupción y que la gran mayoría no tiene el control del proceso de recuperación, adicional a esto se suma el no contar con un esquema de seguridad o no tener el adecuado que se ajuste al negocio, siendo así el nivel de exposición es alto.

Actualmente se confirma que no existen controles de seguridad para protección de información, tampoco existe plan de recuperación en caso de pérdida parcial o total de disponibilidad de servicios, para este trabajo nos enfocamos en el primer obstáculo que es desarrollar e implementar un nivel de seguridad que este alineado a los objetivos y necesidades del negocio. Es responsabilidad de la organización alinearse en tiempo y forma con las buenas prácticas recomendadas y apoyarse con herramientas tecnológicas que faciliten la protección de los activos de la compañía y permitan responder de forma inmediata ante cualquier eventualidad o incidente.

La disponibilidad, integridad y confidencialidad de la información son características que brindan estabilidad a los activos de información y se muestran como un conjunto de condiciones necesarias para mantener un nivel aceptable de seguridad, para lograr cumplir con estas características se debe contar con el compromiso de todo el equipo que forma parte de la organización, desde la presidencia o gerencia hasta el nivel base del organigrama, así también se debe conocer y aplicar técnicas, guías y herramientas actualizados y recomendadas en materia.

Las normas ISO 27002:2013 están enfocadas a brindar un nivel de seguridad idóneo, eficiente y son las bases utilizadas para este proyecto de titulación. Para esto se requirió de un trabajo en equipo con alto compromiso del personal, involucrando la parte administrativa y de tecnología para garantizar la implementación y cumplimiento con los resultados esperados.

1 CAPÍTULO

GENERALIDADES

1.1 ANTECEDENTES

Las empresas tecnológicas deben alinearse a las tendencias y cambios que forman parte del negocio y prever cualquier probabilidad de afectación en los distintos niveles de servicio, principalmente en el que pueda afectar al cliente. La empresa “SGD” para la cual se realiza este estudio ofrece servicios y equipos de tecnología relacionados principalmente a procesos de impresión y gestión documental con el objetivo de mejorar la infraestructura del cliente permitiendo reducir costos, así como el impacto ambiental, mediante el apoyo de herramientas y equipos con características específicas para cada proceso.

Para lograr cumplir con el objetivo de la empresa es de vital importancia mantener registros actualizados de los clientes, así como registrar el contacto principal para realizar seguimiento, validar historial de negociaciones y análisis de posible venta, convirtiéndose toda esta información en la principal fuente de valor.

Los procesos que ejecuta la empresa en relación al negocio como registro de clientes, contratos de mantenimientos, servicios por administración y manejo de Outsourcing, ingreso de activos en bodega, seguimiento a clientes, facturación, proyecciones de ventas, genera la base de clientes, a la cual personal de ventas tiene libre acceso de modificación, a través de la interfaz de usuario, sin nivel de restricción y por ende pueden ser vulnerados con mayor facilidad sin infringir directamente una política, la cartera de clientes es algo muy valioso y está expuesta a la manipulación, divulgación de información no autorizada.

La ausencia de controles de seguridad muestra la falta de concientización sobre protección y genera una idea sobre el nivel de exposición ante cualquier amenaza.

1.2 DESCRIPCIÓN DEL PROBLEMA

Al momento se ha detectado algunos problemas originados por amenazas internas, falta de identificación de vulnerabilidades, ausencia de controles de seguridad para mitigar riesgos asociados a dichas amenazas, desconocimiento del nivel de exposición por el riesgo inherente a los componentes y plataformas tecnológicas en uso.

Entre los problemas detectados se exponen los siguientes:

- Daño en la base de datos que contiene información de clientes, ocasionado por fallas eléctricas.

- Acceso y manipulación de información por parte de usuarios no autorizados en herramienta de gestión de ventas.

- Infección de virus de forma recurrente en la mayoría de las estaciones de trabajo a través de medios de almacenamiento externo y adjuntos de correo.

- Afectación a la función de correos electrónico corporativo por spam y servicio de correo en lista negra.

- Modificaciones al sistema de facturación e inventario, no probados.

- Falta de control sobre los activos existentes, inventarios desactualizados.

- Daño parcial o total del activo durante el almacenamiento y transporte del mismo.

- Falta de mantenimiento y actualizaciones a equipos, herramientas administrativas y aplicaciones.

1.3 SOLUCIÓN PROPUESTA

Dado la problemática presentada sobre la ausencia de políticas y controles de seguridad, se pueden proponer las siguientes recomendaciones basadas en las siguientes categorías de la norma ISO 27002; seguridad y operaciones, control de acceso, seguridad en adquisición y desarrollo de Software, administración de activos, administración de cambio.

Los controles propuestos deben ser revisados y aprobados por gerencia antes de ser implementados y luego de ello se debe evaluar el efecto de los cambios aplicados para comprobar mitigación de los riesgos:

- ✓ En la categoría seguridad y operaciones, se debe revisar el proceso de respaldo de información, para respaldos debe ser considerado la frecuencia, método, comprobación de integridad de información respaldada, ubicación de almacenamiento de respaldo, protección de información respaldada de ser posible cifrar la data para garantizar su confidencialidad, así como la eliminación de los mismos posterior a la confirmación de su expiración.

  Para mitigar el riesgo de infección por malware se tiene que habilitar escaneo de files enviados o recibidos a través de la red o dispositivos externos, para esta tarea se recomienda el uso y configuración de una solución de antivirus con administración centralizada. Se debe habilitar monitoreo de eventos para servidores críticos, se tiene que establecer responsables de identificar posibles vulnerabilidades que puedan afectar estos servidores y acordar un tiempo sobre el manejo de las mismas.

  Adicional para ayudar a contrarrestar la amenaza de interrupción por falta de mantenimiento se propone la instalación de parches para sistema operativo y productos instalados pertenecientes al mismo

fabricante, se sugiere utilizar de forma centralizada la herramienta de actualización WSUS (Windows Server Update Services).

- ✓ En la categoría control de acceso: Revisión, validación y análisis de permisos existentes para usuarios en aplicativos de escritorio, adicional revisión de privilegios a nivel dominio y recursos compartidos de información. Este control se puede manejar a través de administración de políticas centralizadas que vienen embebidas en los controladores de Dominio, políticas de caducidad de passwords para usuarios, validación de últimos passwords utilizados, forzar el cambio de contraseña luego del primer logon para usuarios nuevos o que se reincorporan posterior a periodo determinado, mejorar opciones de complejidad de password, protección de escritorio luego de determinado tiempo de inactividad.

- ✓ En la categoría seguridad en adquisición y desarrollo de Software: Controlar los cambios requeridos para mejora de software de apoyo, organizar los cambios en horarios de menor uso y revisarlos previos a la ejecución.

- ✓ En la categoría seguridad en Comunicaciones: Escanear todos los documentos adjuntos enviados y recibidos vía mail con la ayuda de

antivirus o alguna otra herramienta especializada, controlar y restringir configuraciones que expongan la integridad del servicio de correo o servidor, estar pendientes de boletines de seguridad sobre nuevas vulnerabilidades detectadas por el fabricante del gestor de correo a nivel de cliente, así como las que se detecten a nivel de servidor o aplicativo.

Concientizar y socializar al usuario sobre la recepción, respuesta o envío de algún correo extraño o inusual con indicios de infección de malware que pueden generar como consecuencia envío y recepción de spam.

- ✓ En la categoría administración de activos: Inventariar los activos de la empresa, clasificarlos y revisar periódicamente los accesos a ellos, asegurar el manejo correcto cuando el activo es transportado, eliminado o destruido, protección de información copiada, control de acceso a medios de almacenamiento externos en servidores críticos, control del nivel de accesibilidad y confidencialidad a través de cifrado para información crítica que se maneja de forma externa y es propiedad de la empresa, aplicar copias en medios distintos para evitar problema de acceso por degradación del medio.

- ✓ En la categoría Seguridad Física y Ambiental: Revisar las condiciones físicas y del entorno para prevenir el acceso físico y cualquier daño en las instalaciones donde residan los activos de la información.

1.4 OBJETIVO GENERAL

Diseñar e implementar un esquema de seguridad de nivel 0 a nivel 1 basado en normas ISO 27002:2013 con la finalidad de ofrecer un marco de protección consistente y ajustado a las necesidades de la compañía para mitigar y minimizar los riesgos existentes relacionados al negocio.

1.5 OBJETIVOS ESPECÍFICOS

- ➢ Realizar el levantamiento de información con un departamento de tecnología.
- ➢ Evaluar el nivel de seguridad informática en la infraestructura actual.
- ➢ Identificar los riesgos existentes basados en los resultados de la evaluación previa.
- ➢ Diseñar e implementar políticas y controles de seguridad informática relacionados con la estrategia de negocio.
- ➢ Analizar el resultado posterior a la implementación del esquema de seguridad informática.

1.6 METODOLOGÍA

La solución propuesta se basa en una metodología reconocida y recomendada para implementación de un SGSI (Sistema de Gestión de Seguridad Informática) alineados a norma ISO 27001, en este caso se aplicaría el modelo PHVA (Planificar, Hacer Verificar, Actuar), el objetivo de implementar esta metodología es mantenerse siempre en vanguardia y constante mejora de los controles aplicados con la finalidad de mantener una magnitud de riesgos aceptables y que puedan ser gestionados de una forma eficiente. [1]

El alcance de la solución abarca todos los procesos PHVA, que se detallan a continuación:

Planificar

- ✓ Definir el alcance, objetivos y políticas de seguridad en la organización.
- ✓ Determinar los procesos y sus respectivas secuencias de seguridad, así como los responsables de dichos procesos
- ✓ Definir monitoreo, medición y requerimientos relacionados a seguridad.

Hacer

- ✓ Implementar acciones para alcanzar las actividades planeadas y los resultados deseados.
- ✓ Determinar los recursos necesarios para la operación efectiva de cada proceso.

Verificar

- ✓ Evaluar la eficiencia y aplicación de los controles aplicados.
- ✓ Ajustar de ser necesario los controles o procesos implementados.

Actuar

- ✓ Analizar los resultados de las pruebas y compararlos versus los objetivos de seguridad.
- ✓ Los controles o mejoras deben quedar implementadas de forma oficial siempre y cuando reflejen el resultado esperado.
- ✓ Posterior a un periodo establecido se debe volver al primer punto para para analizar nuevas mejoras a implementar.

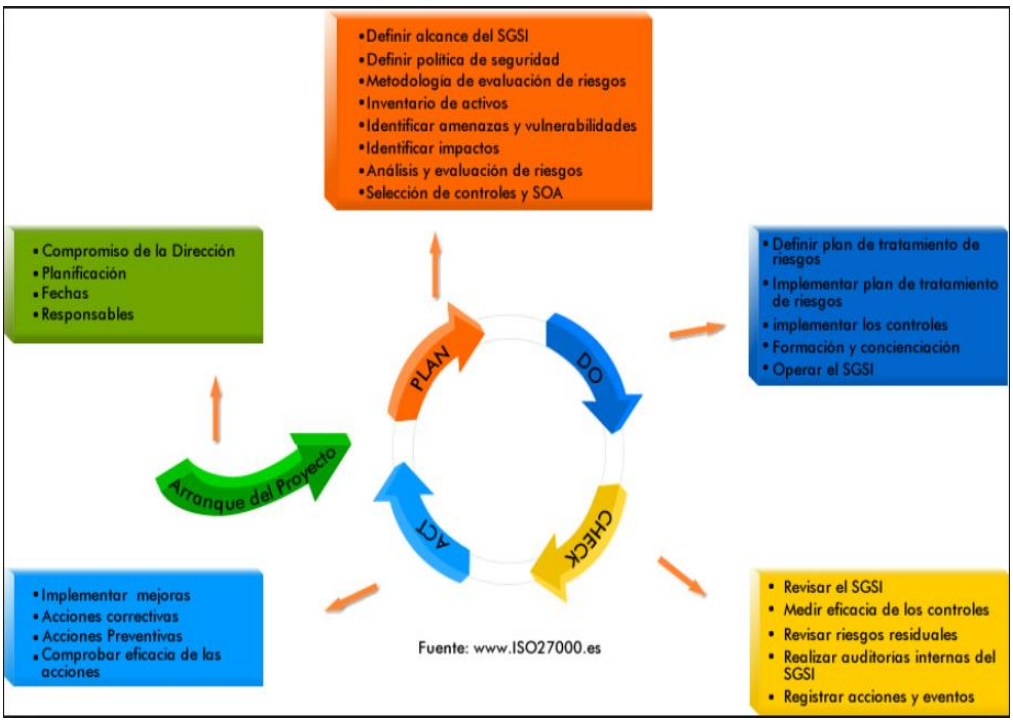


Figura 1.1 Método PHVA Fuente: http://www.iso27000.es

2 CAPÍTULO

MARCO TEÓRICO

2.1 Seguridad Informática

La implementación de cualquier nivel de seguridad informática propone controles, monitoreo y medidas de prevención que se despliegan sobre la infraestructura lógica y física del procesamiento de información.

La seguridad informática es reconocida como el pilar fundamental para la protección de la infraestructura ante una situación en la que se expone la integridad de cualquier activo de información de forma voluntaria o deliberada, el objetivo principal es salvaguardar los activos de información involucrados en el procesamiento de datos y que manejen datos críticos.

La aplicación de seguridad refleja mediante controles y políticas aprobadas y establecidas en pro del negocio, el compromiso de la administración en proteger la imagen y los fines lucrativos de cualquier organización.

Figura 2.1 Seguridad de la Información Fuente: https://www.isotool.org

2.2 ISO 27002

La organización internacional de estandarización, quienes en conjunto con la comisión internacional electrotécnica diseñan, desarrollan, normas según las necesidades reconocidas y expuestas por un grupo conformado por miembros de distintos países, quienes se reúnen anualmente en la sede principal en la ciudad de Ginebra-Suiza y definen estrategias para el desarrollo de alguna posible mejora o nueva norma.

Figura 2.2 Familia ISO 27000 Fuente: es.slideshare.net

La implementación de estas guías reconocidas y aplicables a nivel mundial en cualquier organización, ofrecen un nivel aceptable de administración y protección de los datos en relación a la seguridad, brindando mayor confiabilidad y competitividad en un mercado creciente y dinámico.

En septiembre del 2013 ISO realiza la publicación de un conjunto de recomendaciones y mejores prácticas para establecer y mantener un nivel óptimo de seguridad, esta publicación la realizan dentro de la serie 27000 y corresponde a la versión 27002, esta guía es publicada con un alcance amplio, es decir, sin restricción de uso por parte de cualquier organización, este conjunto de recomendaciones puede ser aplicado de forma parcial o completa por cualquier organización, dependerá únicamente de la cláusula y sus respectivos controles seleccionados acorde al nivel de seguridad deseado, es oportuno mencionar que la aplicación ya sea parcial o completa de esta norma no brinda certificación a diferencia de la norma ISO 27001.

Las cláusulas de control de seguridad incluidos en la norma ISO 27002 son 14 y se listan a continuación.[8]

1. Políticas de Seguridad de la Información
2. Organización de la Seguridad de la Información.
3. Seguridad de los Recursos Humanos.
4. Administración de Activos.
5. Control de Accesos.
6. Cifrado
7. Seguridad Física y Ambiental.
8. Seguridad de Operaciones.
9. Seguridad de Telecomunicaciones.
10. Adquisición, Desarrollo y Mantenimiento de Sistemas.
11. Relación con Proveedores.
12. Gestión de Incidentes de Seguridad de la Información.
13. Aspectos de seguridad de la información en la gestión de continuidad del negocio.
14. Cumplimiento.

2.3 Administración de información como Activo

La información de una organización como activo en la actualidad refleja un nivel alto de criticidad pues representa un pilar fundamental para generación de estadísticas, proyecciones, análisis y posterior toma de decisiones, estos datos hacen referencia a detalles claves del negocio

que para una empresa de ventas de servicios incluye información de cartera de clientes, montos de facturación, inventario, entre otros.

Hoy en día la información que se genera producto de las transacciones y procesos automatizados va aumentando dada la intervención y despliegue de tecnologías y componentes que se logran integrar facilitando la elaboración de flujos de trabajo con diseños flexibles y escalables, procesando información de manera volumétrica y a gran velocidad, ejemplo de lo mencionado podemos citar transacciones en plataformas web, a través de plataformas personalizadas, convenios con entidades, comercios, etc. Por otra parte, se debe tener claro que toda la información indistintamente de su origen o forma de procesamiento debe ser protegida en cada fase y el nivel de protección debe ir acorde a la criticidad que representa en cada etapa de la operación.

De acuerdo al conjunto de recomendaciones y mejores prácticas planteadas en la guía de ISO 27002, se tiene como referencia la aplicación de controles y protección de información, así como su identificación y clasificación por criticidad, medio de uso, método de transferencia, almacenamiento, transporte, método de destrucción cuando la información llegue al final de su vida útil, identificación de responsables internos y externos, compromisos para salvaguardad el procesamiento o administración de información y el activo asociado.

2.4 Vulnerabilidad, Riesgo y Amenaza Informática

Para el diseño y elaboración de controles y políticas se deben conocer las vulnerabilidades, riesgos y amenazas asociadas a los procesos e infraestructura del negocio, se debe tener claro la identificación de cada sección para establecer un control adecuado y analizar el impacto de una forma acertada, con esta acción se logrará coherencia y eficacia con el nivel de protección de la información.

Vulnerabilidad: Es la debilidad de un activo ya sea hardware o software que puede ser explotada por una amenaza para materializar un daño sobre cualquier activo.

Una vulnerabilidad puede reflejarse en aspectos físicos, organizacionales, procedimentales, personales, de administración, de allí parte el criterio de calificación de la vulnerabilidad por el nivel de severidad, así como la prioridad para el proceso de remediación.

La existencia de una vulnerabilidad no siempre genera un riesgo, pues puede darse el caso que no exista una amenaza asociada, por lo tanto, no requerirán de un control, se debe tener claro que el desarrollo de un control errado o el mal uso puede originar una vulnerabilidad. [1]

Riesgo: Se puede definir como una estimación del grado de exposición posiblemente por la materialización de una amenaza sobre uno o varios activos de información, el riesgo permite conocer un impacto estimado en caso de que alguna amenaza se concrete. [2]

Existen formas de tratamiento de riesgos propuestos en la norma ISO 27001 que ayudan a implementar un Sistema de Gestión de Seguridad lo suficiente robusto para poder manejar los riesgos de forma aceptable.

Existen cuatro opciones para tratar los riesgos de las cuales el equipo de trabajo responsable debe seleccionar las mejores teniendo en consideración criticidad y aceptación del riesgo por parte de la empresa, a continuación, se detallan las posibles opciones de tratamiento:

- Disminuir el riesgo a través de aplicación de controles.
- Transferir el riesgo, es decir, trasladarlo a un tercero, pudiendo ser un proveedor o empresa aseguradora.
- Evitar el riesgo, se realiza la omisión del proceso o exclusión del activo que genera el riesgo.
- Aceptar el riesgo, se acepta la existencia del riesgo conociendo que no representa un daño de gran impacto a la empresa, se puede considerar que si el mismo ocurriera se tuviera el ambiente controlado sin alguna situación de lucro cesante o de imagen corporativa. [3]

Amenaza Informática: Se define como amenaza a la posible causa de un incidente que puede afectar a un activo ya sea hardware o software y que pudiera materializarse en cualquier nivel de la organización.

La amenaza informática puede ser causada por factores internos o externos, cuando son externos se originan de forma intencional y por lo general aprovechan una vulnerabilidad en algún componente físico o lógico. Cuando la amenaza es interna, puede ser por alguna falta de control en determinado proceso, error humano no intencional, acto deliberado y con intención de daño severo por parte de algún colaborador. [9]

2.5 Análisis y Gestión de Riesgos

Para la aplicación de controles y políticas eficientes se debe conocer en primera instancia lo que se debe proteger y que tan relevante puede ser para el negocio, siendo así se debe realizar la identificación y tasación para cada activo y conocer el rol del mismo.

En el proceso de análisis de riesgo se busca identificar las vulnerabilidades asociadas a los activos de información y la posibilidad que las mismas se materialicen a través de amenazas, este proceso se logra clasificando los activos de acuerdo a su naturaleza y realizando una tasación de activos en las tres dimensiones propuestas por Magerit.

Los controles de seguridad aplicables dependerán de los resultados de la evaluación cualitativa de riesgos en donde se mostrará la probabilidad e impacto, con esa base se podrán considerar varias acciones de tratamiento detalladas en la definición de Riesgo de la sección anterior: [10]

- ✓ Disminuir el Riesgo.
- ✓ Evitar el Riesgo.
- ✓ Transferir el Riesgo.
- ✓ Aceptar el Riesgo.

2.6 Métodos de Análisis y Gestión de Riesgo

Existen varios métodos para realizar gestión de riesgo aplicables a seguridad informática, entre los más usados están Magerit y OCTAVE que son elegidos con mayor frecuencia por brindar mecanismos de control eficientes; sin embargo, cada uno cuenta con diferentes estructuras reflejadas en el alcance de su aplicación, para el caso de este estudio se hace una comparación resaltando lo más relevante que se ajuste a este trabajo; sin embargo, el método seleccionado es Magerit.

2.7 Método Magerit:

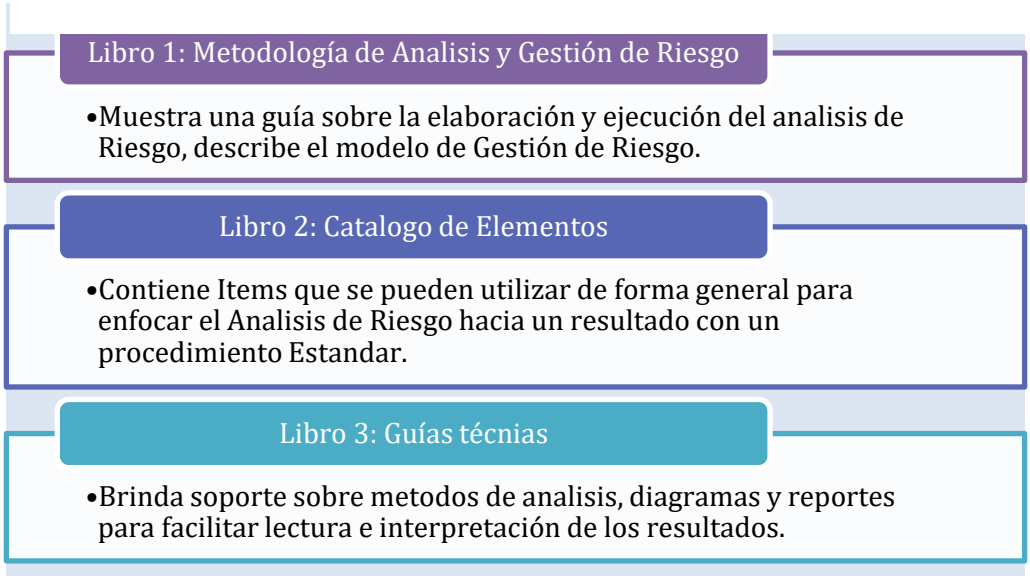
Se define como un “Proceso de Gestión de Riesgo” enfocado en un marco de trabajo para que los entes de Gobierno y Administración tomen decisiones teniendo claridad sobre los riesgos derivados del uso de tecnologías y sistemas de información.

Desde la perspectiva de Magerit se tiene 5 dimensiones de seguridad, de las cuales las primeras tres se aplican de forma general a los datos y las dos últimas ayudan a tener mayor visibilidad sobre las actividades del usuario: [4]

- Disponibilidad: Disposición de los servicios para cuando sean necesarios.
- Integridad: Datos completos y correctos.
- Confidencialidad: Acceso solo a personal autorizado.
- Autenticidad: Confirmación de identidad origen y destino.
- Trazabilidad: Aseguramiento de rastros de cualquier ente que realice cambios.

Esta metodología está compuesta de tres libros con distintos objetivos que se complementan entre sí generando valor en donde se apliquen y creando un punto de partida encaminando a la empresa a la certificación.

Tabla 1: Estructura Magerit



El método Magerit como parte del proceso de análisis y gestión de riesgo presenta dos formas de estudio aplicables de acuerdo a lo que se requiera evidenciar en aspectos intangibles o tangibles:

2.8 Análisis Cualitativo:

Este tipo de análisis ofrece una visión intangible, es decir, no tiene asociado en su aplicación un costo ya que los criterios de evaluación tienen como referencia: [11]

- La imagen de la empresa.
- Cumplimiento de Normativas.
- Capacidad de Operar.
- Nivel competitivo.

2.9 Análisis Cuantitativo:

Este tipo de análisis cuantifica en valor monetario sobre el impacto de la amenaza hacia un activo o proceso y por consecuencia permite analizar si la salvaguarda pudiera aplicarse considerando que la misma no debe exceder el costo de dicho impacto, en este tipo de análisis permite categorizar de forma más precisa que la cualitativa la afectación económica que puede generarse si una amenaza se llegara a materializar. [11]

2.10 Método Octave:

El método en mención tiene a su vez tres tipos de categorías que pueden ser aplicados dependiendo de la dimensión de la empresa objeto de estudio y de acuerdo al alcance de seguridad que se desee brindar.

Este método tiene como alcance la evaluación de Hardware, software, Datos y personas involucradas de acuerdo a la siguiente clasificación.

Tabla 2: Tipos de Métodos Octave

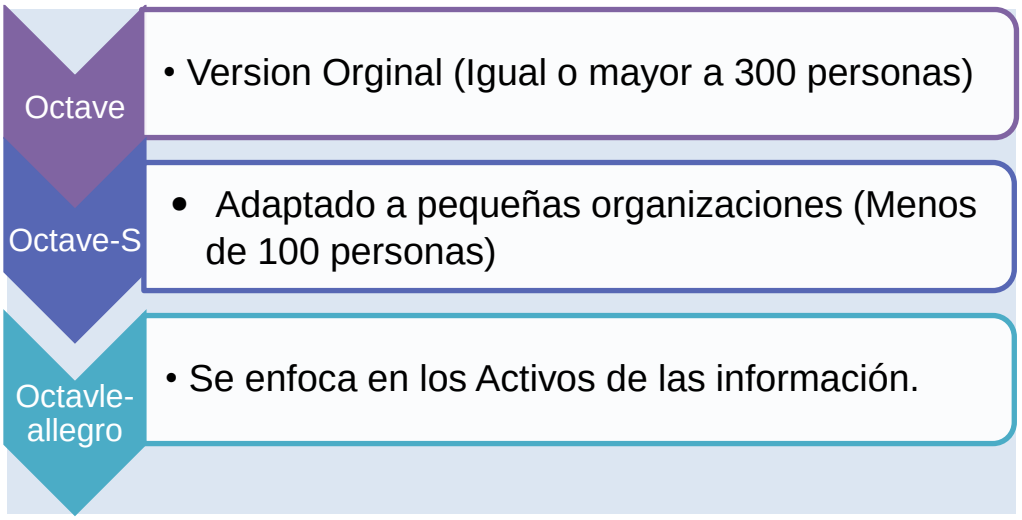


Tabla 3: Comparación Métodos Magerit y Octave

Aspecto	Magerit	Octave
Definición	Metodología elaborada por el consejo Superior de Administración Electrónica, con la finalidad de análisis y gestión de riesgo de sistemas de información.	Se define como una técnica de planificación y consultoría en seguridad basada en el riesgo.
Objetivo	*Concientizar a los responsables de la organización sobre riesgos y la necesidad de gestionarlos. *Ofrecer un método sistemático para el análisis de riesgo por uso de tecnologías. *Ayudar a descubrir y planificar el tratamiento adecuado para controlar el riesgo. *Preparar la organización para procesos de auditoria, acreditación, según sea el caso.	* Permite la comprensión del manejo de recursos. * Identifica y evalúa riesgos que afecten a la seguridad de la organización. * Exige evaluación de la organización y del personal de tecnología de la organización.
Fases	*Presenta conceptos informalmente. *Formaliza las actividades de análisis de riesgo. *Describe opciones de tratamiento de riesgo. *Ejecución de proyectos de análisis de riesgo. *Plan Estratégico y desarrollo de sistemas de Información *Anticipo de problemas que se muestran de forma recurrente en el análisis de riesgo.	Se enfoca en tres fases Identificando información en tres niveles: -Gerencial. -Operacional. -Usuario Final Estos pasos dan lugar a otros 5 para completar los 8 pasos Octave.
Métodos/ Tipos	El Método Magerit viene distribuido en tres libros: *Método. *Catálogo de elementos. *Guía Técnica.	Existen tres métodos independientes: -Octave (Empresa de 300 personas) -Octave-s (Empresas de 100 personas). -Octave Allegro
Características	*Escala de valores cualitativos y cuantitativos. *Prepara a la organización para certificación, acreditación, etc. *Alineada a normas ISO.	*Estudia la infraestructura de la información. *Es Autodirigido. *Es Flexible.

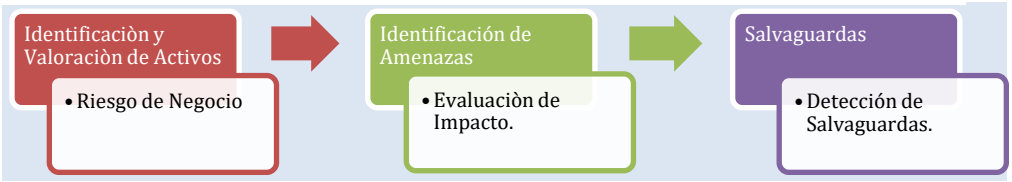
2.11 Pasos de Análisis de Riesgo

De acuerdo a lo expuesto por Magerit, propone una secuencia de pasos para realizar el análisis de riesgo y de tal manera tener encasilladas de forma coherente todas las actividades que se generen durante el ejercicio:

- **Identificación de Activos** con su respectiva clasificación de valor cualitativo para la organización.
- **Identificar las amenazas** a las que están expuestos los activos identificados en el punto anterior.
- **Identificación de Vulnerabilidades** asociadas a los activos y procesos de la organización.
- **Estimar el posible daño** sobre el activo o posible materialización de la amenaza – Evaluación del Impacto.
- **Clasificar los riesgos identificados**.

Las funciones identificadas para la sección de análisis de riesgo se muestran a continuación:

Tabla 4 : Esquema para Análisis de Riesgo



2.12 Políticas de Seguridad Informática

La política de seguridad, son los lineamientos establecidos por la organización, las políticas son aplicadas de acuerdo a las necesidades de seguridad que se identifiquen en el análisis de riesgo y deben ser socializadas y cumplidas por todos los miembros involucrados en el

proceso y que forman parte o brindan algún tipo de servicio a la organización.

Se determina un responsable por la seguridad de la información de igual manera se establece compromisos por los líderes de otras áreas como garantía para el cumplimiento de las normas.

Es recomendable realizar evaluaciones periódicas para validar que el alcance de las políticas protege los activos y procesos críticos y mantiene en un nivel aceptable los riesgos basados en nuevas tendencias o implementaciones tecnológicas.

La política de seguridad debe quedar formalizada, debe estar escrita y las modificaciones que se realicen deben ser comunicadas y aprobadas por gerencia con la finalidad de transparentar y dar a conocer el lineamiento de las políticas en favor del objetivo de la organización. [5]

3 CAPÍTULO

IDENTIFICACIÓN DE NECESIDADES Y LEVANTAMIENTO DE INFORMACIÓN

3.1 Antecedente de la empresa

La empresa “SGD” cuenta con 20 años de experiencia en el mercado, su portafolio inicial solo ofrecía soluciones de servicios de administración en impresión y gestión documental representando de forma oficial a la multinacional Xerox como concesionaria en Guayaquil, la evolución de tecnología para equipos y servicios de impresión desde ese tiempo a la actualidad ha obligado a realizar cambios estratégicos adoptando nuevos productos, siendo ahora un canal mutilimarca que ofrece de forma adicional: ventas de computadoras y equipos a fines, instalaciones para los equipos ofrecidos, contratos de mantenimiento preventivo y

correctivo. Al ser una empresa que ofrece servicios de tecnología su principal actividad es la venta de dichos servicios.

La actividad comercial de esta empresa inicia con el ejercicio que realizan los especialistas en venta mediante el cual elaboran una proyección de sus ventas basada en su cartera de clientes asignada, en consecuencia, la gerencia de ventas establece compromisos de cumplimiento y mide productividad de su equipo.

La Gerencia de ventas realiza la asignación de los clientes para los ejecutivos de esa sección, adicional brinda soporte y acompañamiento durante el proceso de negociación para la mayoría de los casos.

En conjunto con la herramienta que da soporte a ventas se tiene el software de gestión de inventarios y facturación, para estos dos últimos casos utilizan la misma aplicación.

Para el control de asistencia técnica y soporte por contrato de mantenimiento y garantía no se tiene un sistema propio, más bien se utiliza herramienta del canal representado a través de una VPN y por el cual reportan la novedad para posterior programación de soporte, en el caso de que el soporte requerido no este cubierto por garantía con fábrica se utiliza registro local en herramientas de ofimática.

El equipo técnico responsable del proceso de instalación de los equipos y despliegues de las soluciones ofertadas tienen asignada también la

responsabilidad del mantenimiento y soporte de primer nivel de la infraestructura tecnológica de “SGD”.

La infraestructura se encuentra comprometida desde el aspecto físico, económico y de imagen institucional, por el uso de sistemas de información para la gestión de ventas, administración de inventario, facturación, sin niveles mínimos recomendados de protección.

3.2 Estado actual de la empresa en seguridad informática.

Los puntos mencionados en la sección anterior evidencian el nivel de importancia en el soporte a los sistemas de venta, facturación, activos y otras herramientas de tecnología demandadas con frecuencia diaria para el cumplimiento de las tareas.

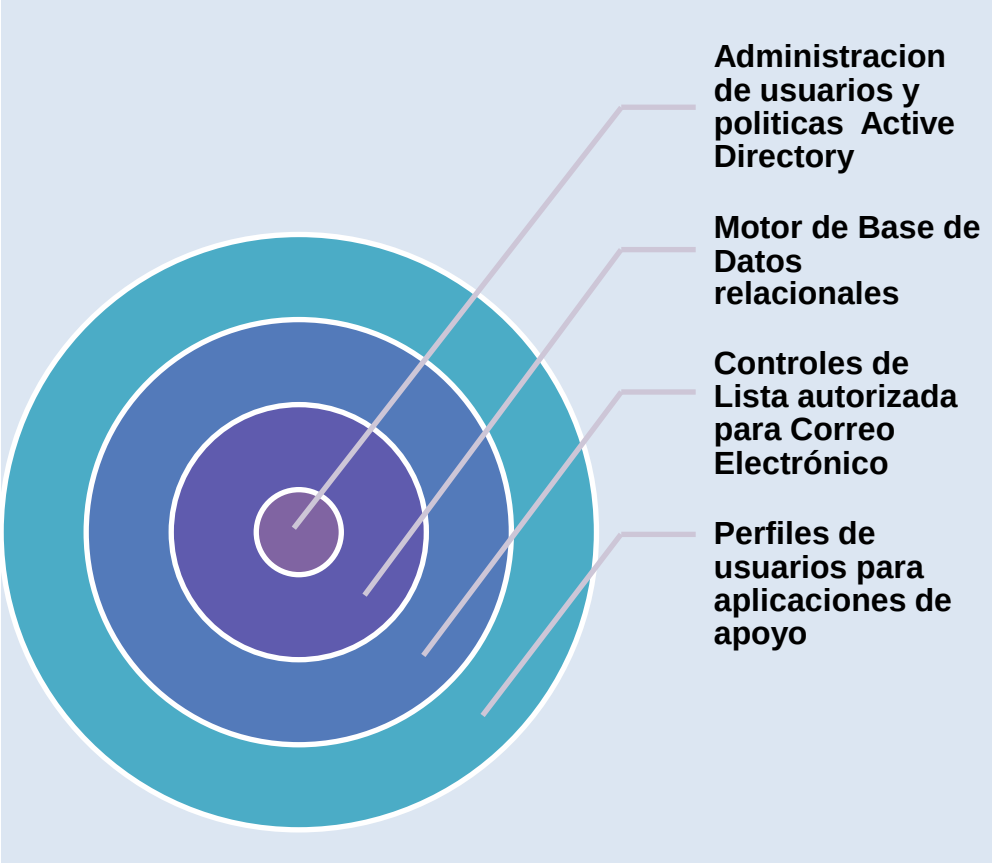
La falta de controles de seguridad establecidos formalmente evidencia lo vulnerable y desprotegido que se encuentra la infraestructura tecnológica, existe una alta probabilidad de daños severos e irreparables como son la pérdida parcial o completa de información a nivel de base de datos de clientes, afectación al sistema de inventario, y demás componentes de apoyo.

Se tiene registro por parte del personal de soporte que se han presentado incidentes sobre la infraestructura y que ha sido difícil la recuperación de los servicios afectados, ya sea por falta de herramientas, procedimientos

o por no tener claridad en el método de recuperación, para poder contrarrestar esta situación han surgido medidas paliativas que por falta de seguimiento y por su naturaleza en sí han perdido consistencia posterior a su aplicación generando una cortina de humo ante los expuestos que se acumulan en el transcurso del tiempo.

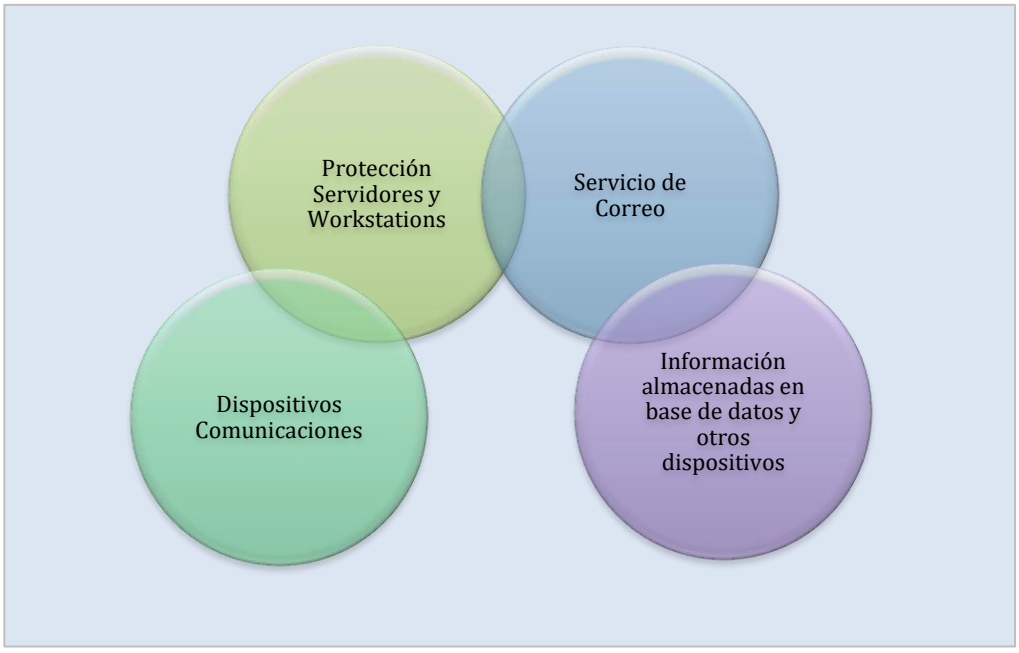
Se lista la estructura que demuestra un mayor nivel de exposición pese a que se tiene opciones de configuración que permiten el afinamiento para robustecer su nivel de seguridad de forma individual y lograr mayor estabilidad y disponibilidad.

Tabla 5: Estructura de Componentes en la infraestructura actual



Por otro lado, existen componentes críticos los cuales deben ser tratados con herramientas diseñadas para tal uso, así poder integrarse con las opciones disponibles y que son configurables a nivel de seguridad para balancear el nivel de protección y disminuir el expuesto, así como, las vulnerabilidades asociadas, por ejemplo: la existencia de malware, protección de comunicaciones externas, protección de activos e información asociada, respaldos, etc.

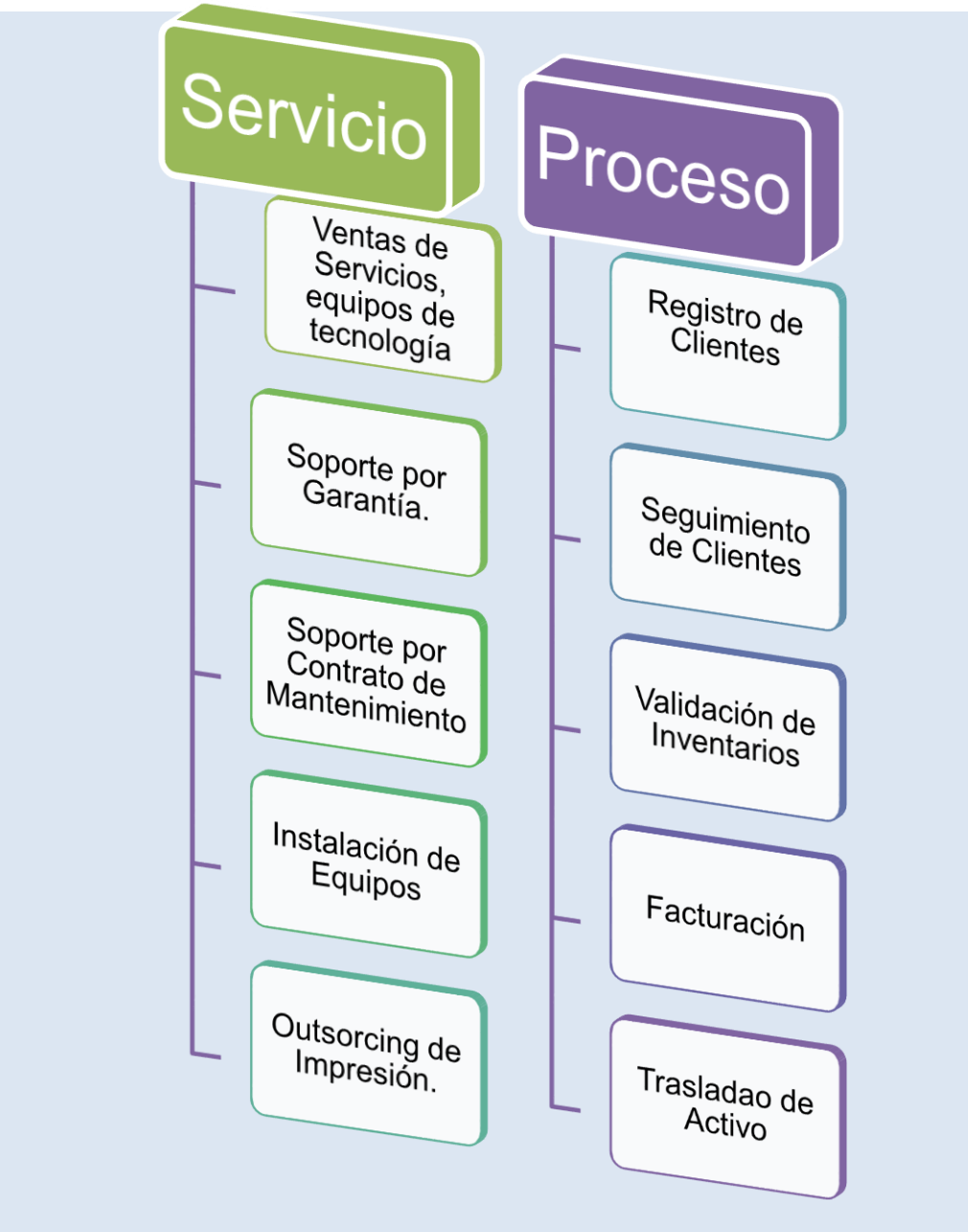
Tabla 6: Componentes que requieren Herramientas Externas



3.3 Identificación de los procesos y servicios críticos.

Los servicios y procesos críticos y que son de vital importancia para la operación de forma ininterrumpida e integra de la compañía se muestran en el siguiente esquema, el orden en el que se muestran no representa la prioridad del proceso o servicio:

Tabla 7: Esquema de Servicios y Procesos



A continuación, se muestra de forma general el flujo común de negociación de venta de un activo realizado por la empresa, esto en primer servicio descrito en el esquema anterior.

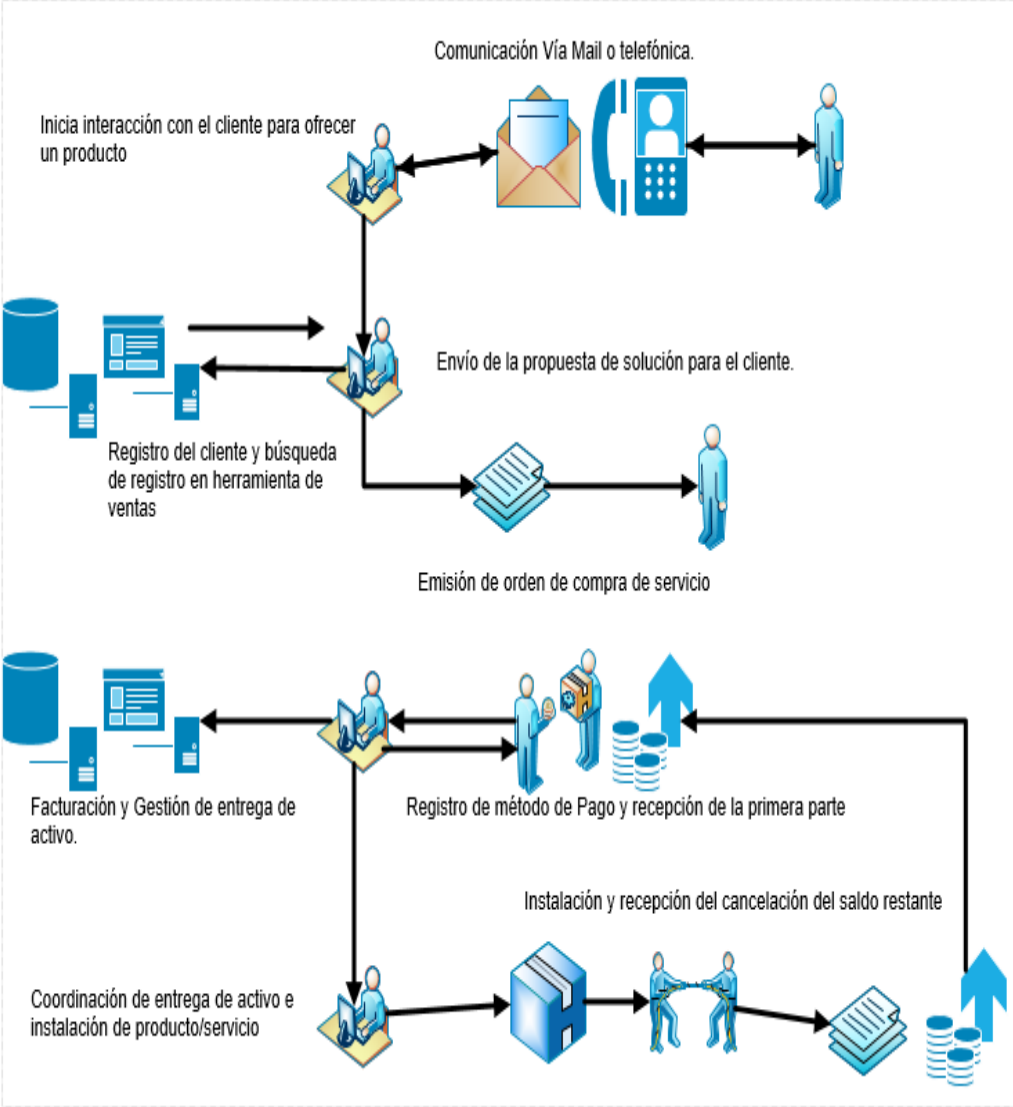


Figura 3.1 Servicio de Venta Fuente: Autor

Este diagrama muestra la infraestructura tecnológica que da soporte a la descripción de la tabla 7, esquemas de servicios y procesos.

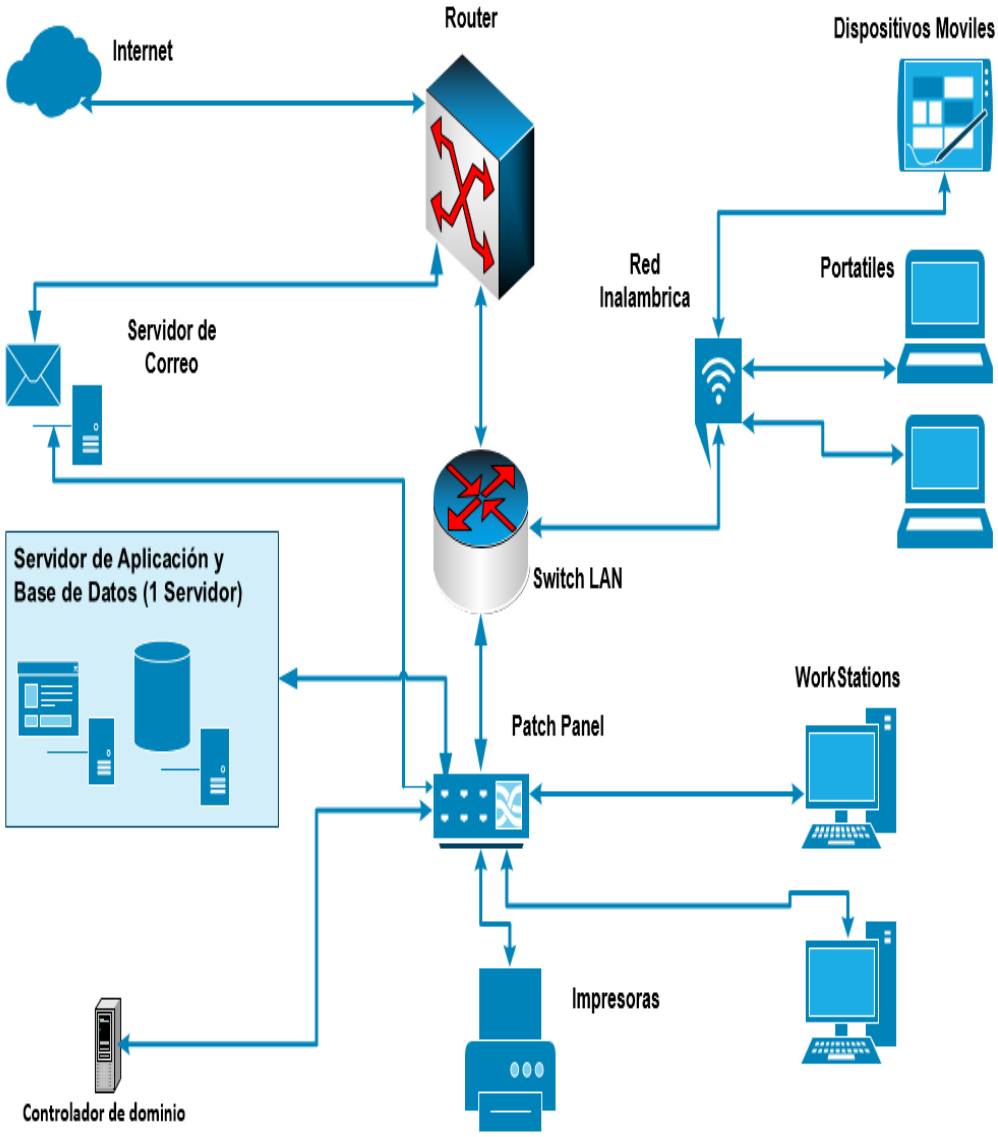


Figura 3.2 Infraestructura de Tecnología Fuente: Autor

3.4 Identificación de Activos

Para poder determinar los riesgos vigentes asociados a la infraestructura tecnológica, así como poder aplicar el mejor tratamiento y control para mitigarlos se debe conocer los activos de información y el valor que representa cada uno.

De acuerdo a la metodología Magerit, los activos esenciales son la información y los servicios prestados, estos a su vez tienen una relación de dependencia con activos prosaicos, es decir, existen activos que tienen una criticidad mayor pero que reflejan dependencia de algún otro activo de menor valor, entonces, la posible afectación o daño podría generarse desde el activo de menor valor afectando al que se encuentre en el nivel jerárquico superior, siendo el nivel de relación lo que represente la magnitud del daño para el activo principal.

Adicional para conocer el valor de los activos se debe establecer las posibles dimensiones sobre las cuales se realizará la valoración, pudiendo ser: confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad.

El método de valoración de cada activo debe ser seleccionado entre las opciones de cualitativo y cuantitativo, ambos descritos en la sección de Magerit en el segundo capítulo de este estudio.

Tabla 8: Identifación de Activos de Información

Cantidad	Activo	Código	Tipo de Activo
1	Servidores Físicos	HW	Hardware y Datos
2	Base de Datos	D	Datos
3	Workstations/Laptops	HW	Hardware
4	Impresoras	HW	Hardware
5	Dispositivos Almacenamiento Externo	M	Media
6	Dispositivos de Comunicación-redes	COM	Hardware/Comunicación
7	Vehículo/Transporte	L	Vehículo
8	Dispositivos externos de almacenamiento	HW	Hardware
9	Cámaras – Vigilancia	AUX	Hardware
10	Personal	P	Persona
11	Software de Facturación	SW	Sistema de Información
12	Software de Inventario	SW	Sistema de Información
13	Software de Gestión de Ventas	SW	Sistema de Información
14	Servicio de correo electrónico	S	Comunicación
15	Central IP	COM	Hardware/Comunicaciones
16	Documentos Físicos generados por transacciones	D	Datos

Con la lista de activos de información se procede a realizar la tasación de los mismos aplicando la escala Likert por la facilidad y rapidez en su aplicación y considerando las 3 dimensiones de seguridad utilizadas con mayor frecuencia: disponibilidad, integridad, confidencialidad.

A=Activo

D=disponibilidad

I=Integridad

C=confidencialidad

(3.1)

$$A = \frac{D + I + C}{3}$$

Para este ejercicio utilizaremos la siguiente escala:

Tabla 9: Escala de Likert Fuente: Autor

Nivel	**Valor**
Muy Bajo	1
Bajo	2
Medio	3
Alto	4
Muy Alto	5

Tabla 10: Tasación de Activos Fuente: Autor

Procesos	Código Activo	Activos	Tipo de Activo	D	I	C	A
Registro de Clientes	SW	Software de Ventas	Software	5	5	3	4.33
	HW	Workstation/Portable	Hardware	3	4	4	3.66
	COM	Dispositivos de Comunicación-redes	Hardware	5	4	4	4.33
	P	Ejecutivo de Ventas	Persona	3	5	5	4.33
	S	Servicio de Directorio Activo	Software	5	5	3	4.33
Seguimiento de Clientes	SW	Software de Ventas	Software	5	5	3	4.33
	HW	Workstation/Portable	Hardware	3	4	4	3.66
	COM	Central IP	Hardware /Comunica	5	4	4	4.33
	COM	Dispositivos de Comunicación-redes	Hardware	5	4	4	4.33
	P	Ejecutivo de Ventas	Persona	3	5	5	4.33
	S	Servicio de Correo	Servicio	4	5	5	4.66
Validación de Inventario	SW	Sistema de Inventarios	Software	5	5	3	4.33
	HW	Equipo/parte para Venta.	Hardware	3	3	3	3
	P	Administrador de Logística.	Persona	3	5	5	4.33
	HW	Workstation/portable	Hardware	3	4	4	3.66
Facturación	SW	Sistemas de Inventarios	Software	5	5	3	4.33
	SW	Software de Ventas	Software	5	5	3	4.33
	SW	Sistemas de Facturación	Software	5	5	4	4.66
	HW	Equipo/parte para Venta.	Hardware	3	3	3	3
	HW	Impresora	Hardware	3	1	1	1.66
	D	Factura	Información	5	4	3	4
	D	Base de Datos	Datos	5	5	4	4.66
Traslado de Activo	SW	Sistemas de Inventario	Software	5	5	3	4.33
	HW	Equipo/parte vendida	Hardware	4	5	3	4
	L	Vehículo de Transporte.	Servicio	3	2	2	2.33
	P	Equipo de Logística	Persona	3	5	4	4
	AUX	Cámaras de Vigilancia IP	Hardware	3	3	3	3

3.5 Identificación de riesgos, vulnerabilidades y amenazas.

Los niveles de riesgos existentes generados por amenazas internas o externas y que tienen alta probabilidad de ocurrencia son aquellos que representan el mayor nivel de peligro para el estado de salud de los activos en cualquier dimensión comprometiendo de forma directa a algún servicio de la compañía.

Para poder diseñar e implementar métodos y controles eficientes, se debe conocer los riesgos existentes y la magnitud del impacto que puede afectar a los activos de mayor valor, si bien es cierto es difícil estimar algún daño de forma exacta por ello la mejor técnica de defensa es asumir que puede ocurrir en cualquier momento y tener una opción que mitigue dicho riesgo.

De acuerdo a Magerit la amenaza es una causa potencial de un incidente que puede causar daños a un sistema de información o a una organización [4].

Las amenazas se pueden identificar de la siguiente forma de acuerdo a Magerit:

- Origen Natural: Accidentes naturales (terremotos, inundaciones, etc.).
- Del Entorno: Se derivan de las funciones u acciones que realiza la compañía, pueden ser originados por contaminación, fallos eléctricos,

ante los cuales el sistema de información y activos sufren en menor proporción.

- ❖ Defectos de las Aplicaciones: Se originan de forma natural con el diseño o implementación, las consecuencias son negativas y afectan directamente los sistemas de información.
- ❖ Causadas por las personas: Pueden ser causadas de forma accidental o de forma deliberada. Cuando una persona por omisión o error ejecuta alguna acción sin alguna mala intención se considera que el origen de la amenaza ocurre de forma accidental; sin embargo, cuando las personas tienen acceso a la información pueden causar problemas intencionados con el objetivo de beneficiarse o simplemente causar algún perjuicio actuando de forma deliberada.

La amenaza puede aprovechar una vulnerabilidad y perjudicar a un activo en distintas dimensiones, sin embargo, la afectación no se da en igual proporción, el nivel de influencia de una amenaza sobre un activo se debe valorar en dos sentidos:

- ✓ **Degradación:** nivel de afectación del valor del activo, suele ser representada como una fracción del valor del activo siendo así puede estar parcial o totalmente degradado.
- ✓ **Probabilidad:** El nivel de probabilidad de materialización de la amenaza.

Tabla 11: Amenazas y Vulnerabilidades Fuente: Autor

Activo de Información	Código Amenaza	Amenaza	Vulnerabilidad Relacionada
Software de Ventas	A8.1	Malware	Falta de protección antimalware.
	E19.1	Fuga de Información	Falta de control por acceso a la información.
	O1.1	Operaciones no autorizadas	Privilegios elevados para todos los usuarios.
	E18.1	Pérdida parcial o total de información financiera	Falta de política de respaldos.
Workstation /Portable	E25.1	Pérdida de Equipo	Ausencia de control y registro de inventarios
	E2.1	Pérdida de información total o parcial	Falta de Respaldos para información sensible.
	E8.1	Infección por Virus	Ausencia de Antivirus
	A29.1	Secuestro de información Ransomware	Falta de política de actualización y navegación.
Dispositivos de Comunicación Redes	I6.1	Indisponibilidad por interrupción de suministro eléctrico.	No se tiene fuente redundante para estos equipos.
	E4.1	Daño Lógico por Configuración	No se tiene respaldo de configuración.
	I5.1	Daño Físico que requiere reemplazo total o parcial.	No existe contrato de mantenimiento con este tipo de Cobertura
Ejecutivo de Ventas	A7.1	Uso inadecuado de equipo/computador	Falta de control para correcto uso de dispositivo.
	A29.1	Robo de Información	Falta de controles sobre accesos y privilegios.
	A28.1	Indisponibilidad del Personal	Enfermedad
	A19.1	Divulgación de Información	Falta de Políticas de reserva y no divulgación.
Central IP	I6.1	Daño de central por inconvenientes de energía	Conexiones de energía directas sin protección contra variaciones.
	I8.1	Degradación del servicio a causa de la internet	Solo se tiene un proveedor de internet.
	A7.1	Uso inadecuado de equipos	Falta de conocimiento en la administración de la infraestructura.
	A8.1	Bloqueo parcial o total del servicio.	Afectación por SPAM.

	A5.1	Suplantación de Identidad	Fraude por Pishing.
Servicio de Correo	A8.1	Afectación por Malware	Infección de virus por falta de protección.
	A29.1	Robo de Información	Ataques de Ransomware
	I6.1	Indisponibilidad por interrupción de suministro eléctrico.	Falta de UPS.
	E25	Errores de Mantenimiento	Falta de Mantenimiento
Sistema de Inventario	A8.1	Afectación por Malware	Falta de herramienta de protección corporativa.
	E7.1	Información no actualizada	Deficiencia en controles y registro de mercaderías.
	E7.1	Activos categorizados de forma incorrecta	Deficiente administración de activos.
	E2.1	Pérdida parcial o total de información.	No existe política de respaldos.
Sistemas de Facturación	A8.1	Afectación por Malware	Falta de herramienta de protección corporativa
	E2.1	Pérdida parcial o total de información.	No existe políticas de respaldo.
	E4.1	Cambios sin control de parámetros del sistema por proveedores.	Falta de registro de control de cambios.
Servidor de Base de Datos	A8.1	Afectación por Malware	Falta de herramienta de protección corporativa
	E18.1	Pérdida parcial o total de información	No existe política de respaldo.
	E4.1	No hay control para acceso de usuarios de aplicativos	No existe política de claves para usuarios a nivel de base de datos.
	E23.1	Errores de Mantenimiento	Falta de procedimiento de parchado
Servidor Controlador	A8.1	Afectación por Malware	Falta de herramienta de protección corporativa
	E4.1	Acceso físico y lógico sin control	Ausencia de políticas de acceso y uso.
	E23.1	Errores de Mantenimiento	Falta de mantenimiento
	A11.1	Acceso no autorizado	Falta de Hardenización.
Cámara IP	I1.1	Fenómeno Natural	Exposición de cámaras sin protección.
	E23.1	Errores de Mantenimiento	Falta de Mantenimiento Preventivo.
	A7.1	Uso inadecuado	Dispositivo sin uso por mala configuración.
Inventario/ Activo	E7.1	Listado de activo desactualizado o incompleto	Ausencia de política para manejo de activos
	A7.1	Daños Físico de Activo	Lugar inapropiado de almacenaje.

	E25.1	Pérdida de Activo	Deficiente administración de Activo
Impresora	E4.1	Acceso a través de credenciales por defecto.	Falta de política para usuarios de aplicación
	E23.1	Errores de Mantenimiento	Falta de Mantenimiento Preventivo.
	A7.1	Uso inadecuado de equipos	Poco conocimiento del dispositivo y su configuración.
Administrador de Bodega	A28.1	Riesgo Interno	Uso excesivo de fuerza por manipulación de activo.
	A28.1	Indisponibilidad del personal	Enfermedad
	A7.1	Daño Físico de Activo	Falta de conocimiento en manipulación.
Dispositivos externos de almacenamiento	E19.1	Fuga de Información	Ausencia de política por manejo de información en medios extraíbles.
	A25.1	Robo de Información	Ausencia de políticas por confidencialidad.
	AS1	Infección de malware	Ausencia de controles para revisión periódica de dispositivos externos.

El método de Magerit propone una forma de medición de ocurrencia tomando en consideración un año, de esta manera se puede utilizar el siguiente modelo con los siguientes valores:

Tabla 12: Probabilidad de Ocurrencia, Autor: Magerit Libro I

Código	Descripción	Frecuencia	Valor
MA	Muy Frecuente	Diario	5
A	Frecuente	Mensualmente	4
M	Normal	Una vez al año	3
B	Poco Frecuente	Cada varios años	2
MB	Muy Poco Frecuente	Siglos	1

Tabla 13: Niveles de Aceptación de Riesgo. Fuente: Autor.

Niveles de Riesgo			
Nivel	**Rango**	**Nivel**	**Alcance**
1	1-4.9	Aceptado	No requiere control
2	5-10.9	Bajo	Se debe aplicar controles para llegar a nivel 1
3	11-15.9	Medio	Se debe aplicar controles para llegar a nivel 2.
4	16-25	Alto	Se debe aplicar controles para llegar a nivel 3.

Tabla 14: Evaluación de Impacto y Riesgo. Fuente: Autor

Activo	Valor Activo	No.	Amenaza	Vulnerabilidad	Probabilidad	Riesgo
Software de Ventas	4,33	1	Malware	Falta de protección antimalware.	3	12,99
		2	Fuga de Información	Falta de control por acceso a la información.	3	12,99
		3	Operaciones no autorizadas	Privilegios elevados para usuarios no administradores	4	17,32
		4	Pérdida parcial o total de información financiera	Falta de política de respaldos.	3	12,99
Workstation/ Portable	3,66	5	Pérdida de Equipo	Ausencia de control y registro de inventarios	3	10,98
		6	Pérdida de información total	Falta de Respaldos para información sensible.	4	14,64
		7	Infección por Virus	Ausencia de Antivirus	4	14,64
		8	Secuestro de información Ransomware	Falta de política de actualización y navegación.	1	3,66
Dispositivos de Comunicación	4,33	9	Indisponibilidad por corte de energía	No se tiene fuente redundante para estos equipos.	3	12,99
		10	Daño Lógico por Configuración	No se tiene respaldo de configuración.	2	8,66
		11	Daño Físico que requiere reemplazo total o parcial	No existe contrato de mantenimiento con este tipo de Cobertura	2	8,66
Ejecutivo de Ventas	4,33	12	Uso inadecuado de computador	Falta de control para correcto uso de dispositivo.	3	12,99

		13	Hurto de Información	Falta de controles sobre accesos y privilegios.	3	12,99
		14	Indisponibilidad del Personal	Enfermedad	3	12,99
		15	Divulgación de Información	Falta de Políticas de reserva y no divulgación.	3	12,99
Central IP	4,33	16	Daño de central por inconvenientes de energía	Conexión de energía directas sin protección contra variaciones.	2	8,66
		17	Degradación del servicio a causa de la internet	Solo se tiene un proveedor de internet.	2	8,66
Servidor de Correo	4,66	18	Bloqueo parcial o total del servicio.	Afectación por SPAM.	4	18,64
		19	Suplantación de Identidad	Fraude por Pishing.	1	4,66
		20	Afectación por Malware	Infección de virus por falta de protección.	3	13,98
		21	Secuestro de Información	Ataques de Ransomware	1	4,66
		22	Propagación de infección a través del servicio	Infección por archivos adjuntos.	4	18,64
		23	Acceso no autorizado local.	Falta de Hardenización.	3	13,98
		24	Acceso remoto no autorizado	Seguridad de conexión remota, débil o inexistente	3	13,98
Sistema de Inventario	4,33	25	Afectación por Malware	Falta de herramienta de protección corporativa.	3	12,99
		26	Información no actualizada	Deficiencia en controles y registro de mercaderías.	4	17,32
		27	Activos categorizados de forma incorrecta	Deficiente administración de activos.	4	17,32

		28	Pérdida parcial o total de información.	No existe política de respaldos.	3	12,99
Sistemas de Facturación	4,66	29	Afectación por Malware	Falta de herramienta de protección corporativa	3	13,98
		30	Pérdida parcial o total de información.	No existe políticas de respaldo.	3	13,98
		31	Cambios sin control de parámetros del sistema por proveedores	Falta de registro de control de cambios.	4	18,64
Servidor de Base de Datos	4,66	32	Afectación por Malware	Falta de herramienta de protección corporativa	3	13,98
		33	Pérdida parcial o total de información	No existe política de respaldo.	3	13,98
		34	Afectación al motor de base de datos	No existe proceso de parchado para motor.	4	18,64
		35	No hay control para acceso de usuarios de aplicativos	No existe política de claves para usuarios a nivel de base de datos ni aplicativos	3	13,98
		36	Componentes y servicios desactualizados	Falta de procedimiento de parchado para servidor.	4	18,64
Servidor Controlador de Dominio	4,66	37	Afectación por Malware	Falta de herramienta de protección corporativa	3	13,98
		38	Método de recuperación ante fallos	No existe documentación de la instalación	3	13,98

		39	Acceso físico y lógico sin control	Ausencia de políticas de acceso y uso.	3	13,98
		40	Daño físico o lógico	Falta de mantenimiento y revisiones periódicas.	4	18,64
		41	Servicios no autorizados	Falta de Hardenización.	4	18,64
Cámara IP	3	42	Fenómeno Natural	Exposición de cámaras sin protección.	1	3
		43	Inoperatividad de dispositivos	Falta de Mantenimiento y revisiones periódicas.	3	9
		44	Inoperatividad parcial o total	Funciones sin uso por mala configuración.	4	12
Inventario/Activo	4	45	Listado de activo desactualizado o incompleto	Ausencia de política para manejo de activos	4	16
		46	Daños Físico de Activo	Lugar inapropiado de almacenaje.	3	12
		47	Pérdida de Activo	Deficiente administración de Activo	2	8
Impresora	1,66	48	Acceso a través de credenciales por defecto.	Falta de política para usuarios de administración.	4	6,64
		49	Inoperatividad de dispositivos.	Falta de Mantenimiento Preventivo.	3	4,98
		50	Uso de servicios no autorizados	Poco conocimiento del dispositivo.	3	4,98
Administrador de Bodega	4,33	51	Riesgo Interno	Uso excesivo de fuerza por manipulación de activo.	3	12,99
		52	Indisponibilidad del personal	Enfermedad o Calamidad Domestica	4	17,32

		53	Daño parcial de activo	Falta de conocimiento en manipulación de equipos	3	12,9
Dispositivos externos de almacenamiento	3,66	54	Fuga de Información	Ausencia de política por manejo de información en medios extraíbles	3	10,98
		55	Robo de Información	Ausencia de políticas por confidencialidad.	2	7,32
		56	Infección de malware	Ausencia de controles para revisión periódica de dispositivos externos.	4	14,64

Probabilidad		Impacto			
		Aceptado 1-4.9	Bajo 5-10.9	Medio 11-15.9	Alto 16-25
Muy Frecuente	5				3
Frecuente	4			7, 36	32, 35
Normal	3	50, 51	5, 9, 49, 55	1, 4, 6, 12, 24, 26, 30, 33, 40, 45, 47, 54, 57	18, 19, 23, 27, 28, 37, 41, 42, 46, 53
Poco Frecuente	2			10, 11, 16, 17, 48, 8, 52, 56	2, 9, 13, 14, 15, 21, 29, 31, 34, 39, 44,
Muy poco frecuente	1	8, 20, 22, 43			

Figura 3.3 Mapa de Calor de Riesgo. Fuente: Autor

4 CAPÍTULO

ANÁLISIS, DISEÑO DE POLÍTICAS Y CONTROLES

4.1 Beneficios de la norma ISO 27002.

La norma ISO 27002 establece guías de mejores prácticas a nivel de seguridad y como tal la implementación de esta norma no exige ni prepara a una compañía para certificación, a diferencia de la norma ISO 27001, la norma utilizada en esta solución al igual que las demás son revisadas por expertos de diferentes países con el objetivo de proponer guías y recomendaciones actualizadas a quienes están expuestos a sobrellevar complicaciones a nivel de seguridad y no tener claridad de cómo proceder ante cualquier evento que genere una amenaza.

La aplicación de esta norma da un soporte robusto para la implementación de un Sistema de Gestión de Seguridad de la información y brinda los siguientes beneficios:

- Genera conciencia sobre la necesidad de la seguridad de la información.
- Óptimo control y protección de activos críticos de información
- Propone controles para validación y mejoras de políticas ya establecidas.
- Mejor disponibilidad de servicios de tecnología por prevención y disminución de incidentes.
- Ofrece un alcance y aplicación flexible de tal manera que pueda ajustarse a las necesidades existentes.
- Establece el inicio para la implementación de un SGSI.

Figura 4.1 ISO 27002 Fuente:https://itunes.apple.com/us/app/iso-27002-information-security.

4.2 Gestión y Tratamiento de Riesgos

La sección de gestión y tratamiento de riesgo ayuda a seleccionar la mejor opción de tratamiento para remediar el riesgo identificado basado en el nivel de criticidad del mismo, la intención no solo es la disminución del riesgo, sino conocer el posible impacto que el mismo ocasionaría sobre un activo sino se tuviera definida una opción de remediación. [7]

Las opciones de tratamiento se detallan a continuación:

Reducir el Riesgo: Aplicando controles de seguridad para reducir los riesgos, mejorando procedimientos, actualizando políticas y utilizando herramientas de apoyo se puede lograr cambiar el nivel de riesgo.

Compartir o Transferir el Riesgo: Se logra utilizando un apoyo formal externo, donde se transfiere total o parcialmente la responsabilidad a una empresa con servicio especializado, siendo la figura del proveedor seleccionado el responsable de velar por la disponibilidad e integridad de los activos expuestos en esta categoría.

Eliminar el Riesgo: Se logra eliminando el activo, proceso, procedimiento que pudiera originar el incidente.

Aceptación del Riesgo: Cuando las acciones para eliminar el riesgo exceden el costo de la consecuencia de materialización del mismo o los controles aplicados exceden el límite del presupuesto designado para la aplicación del control, siendo así, resulta mejor convivir con el riesgo y minimizar el impacto, tal vez con la aplicación de pólizas de seguros o utilización de otros recursos de apoyo.

Figura 4.2 Gestión de Riesgo, Fuente:

https://www.ucn.edu.co/programas-academicos/Paginas/posgrados/

4.3 Análisis de políticas y controles requeridos.

Las opciones de tratamiento y controles han sido revisadas y seleccionadas de acuerdo a las necesidades reflejadas en la matriz de riesgo elaborada en el capítulo anterior, se consideraron recomendaciones que forman parte de la guía de controles ISO 27002:2013, a continuación, se adjunta la tabla de análisis y tratamiento de riesgo, en conjunto con la cláusula de control seleccionada.

Tabla 15: Plan de Tratamiento de Riesgo. Fuente: Autor

Activo de Información	Código Amenaza	Amenaza	Vulnerabilidad Relacionada	Opción de Tratamiento	Clausula de Seguridad
Cámara IP	I1.1	Fenómeno Natural	Exposición de cámaras sin protección.	Aceptar	N/A
	E23.1	Errores de Mantenimiento	Falta de Mantenimiento Preventivo.	Reducir	11 Seguridad Física y Ambiental
	A7.1	Uso inadecuado	Dispositivo sin uso por mala configuración.	Reducir	8 Administración de Activo
Dispositivos de Comunicación Redes,	I6.1	Indisponibilidad por interrupción de suministro eléctrico	No se tiene fuente redundante para estos equipos, posible daño en equipo.	Reducir	11 Seguridad Física y Ambiental
	E4.1	Daño Lógico por Configuración	No se tiene respaldo de configuración.	Reducir	12 Seguridad de Operación

Central IP	I5.1	Daño Físico que requiere reemplazo total o parcial.	No existe contrato de mantenimiento con este tipo de Cobertura	Reducir	11 Seguridad Física y Ambiental
	I8.1	Degradación del servicio a causa de la internet	Solo se tiene un proveedor de internet.	Aceptar	N/A
Servidor de Base de Datos	A8.1	Afectación por Malware	Falta de herramienta de protección corporativa	Reducir	12 Seguridad de Operación
	E18.1	Pérdida parcial o total de información	No existe política de respaldo.	Reducir	12 Seguridad de Operación
	E4.1	Acceso a usuarios con claves débiles o por defecto.	No existe política de claves para usuarios a nivel de base de datos.	Reducir	9 Control de Acceso
	E23.1	Errores de Mantenimiento	Falta de procedimiento de parchado	Reducir	11 Seguridad Física y Ambiental
Workstation /Portable, Inventario /Activo,	E25.1	Pérdida de Equipo	Ausencia de control y registro de inventarios	Reducir	8 Administración de Activo
	E2.1	Pérdida de información total o parcial	Falta de Respaldos para información sensible.	Reducir	12 Seguridad de Operación
	E8.1	Infección por Virus	Ausencia de Antivirus	Reducir	12 Seguridad de Operación
	A29.1	Secuestro de Información Ransomware	Falta de política de actualización y navegación.	Reducir	11 Seguridad Física y Ambiental
	E7.1	Listado de activo desactualizado o incompleto	Ausencia de política para manejo de activos	Reducir	8 Administración de Activo
	A7.1	Daño Físico de Activo	Lugar inapropiado de almacenaje.	Reducir	8 Administración de Activo
Impresora.	E4.1	Acceso a través de credenciales por defecto.	Falta de política para usuarios de Administración	Reducir	9 Control de Acceso
	E23.1	Errores de Mantenimiento	Falta de Mantenimiento Preventivo.	Reducir	11 Seguridad Física y Ambiental

	A7.1	Uso inadecuado de equipos	Poco conocimiento del dispositivo y su configuración.	Reducir	8 Administración de Activo
Dispositivos externos de almacenamiento	E19.1	Fuga de Información	Ausencia de política por manejo de información en medios extraíbles.	Reducir	8 Administración de Activo
	A25.1	Robo de Información	Ausencia de políticas por confidencialidad.	Aceptar	N/A
	AS1	Infectación de malware	Ausencia de controles para revisión periódica de dispositivos externos.	Reducir	12 Seguridad de Operación
Ejecutivo de Ventas, Administrador de Bodega	A7.1	Uso inadecuado de equipo/computador	Falta de control para correcto uso de dispositivo.	Reducir	8 Administración de Activo
	A29.1	Robo de Información	Falta de controles sobre accesos y privilegios.	Reducir	9 Control de Acceso
	A28.1	Indisponibilidad del Personal	Enfermedad	Aceptar	N/A
	A19.1	Divulgación de Información	Falta de Políticas de reserva y no divulgación.	Aceptar	N/A
	A28.1	Riesgo Interno	Uso excesivo de fuerza por manipulación de activo.	Aceptar	N/A
	A7.1	Daño Físico de Activo	Falta de conocimiento en manipulación.	Reducir	8 Administración de Activo
Servidor de Correo/ Servidor Controlador	A8.1	Bloqueo parcial o total del servicio.	Afectación por SPAM.	Transfer	Contratar un servicio de protección especial
	A5.1	Suplantación de Identidad	Fraude por Pishing.	Reducir	12 Seguridad de Operación
	A29.1	Robo de Información	Ataques de Ransomware	Reducir	11 Seguridad Física y Ambiental
	I6.1	Indisponibilidad por interrupción de suministro eléctrico	Falta de UPS.	Reducir	11 Seguridad Física y Ambiental

	E25	Errores de Mantenimiento	Falla en funcionamiento de activo	Reducir	11 Seguridad Física y Ambiental
	E4.1	Acceso físico y lógico sin control	Ausencia de políticas de acceso y uso.	Reducir	11 Seguridad Física y Ambiental
	E23.1	Errores de Mantenimiento	Falta de Mantenimiento	Reducir	11 Seguridad Física y Ambiental
	A11.1	Acceso no autorizado	Falta de Hardenización.	Aceptar	N/A
Software de Ventas, Software de Inventario, Software de Facturación.	E19.1	Fuga de Información	Falta de control por acceso a la información.	Reducir	9 Control de Acceso
	O1.1	Operaciones no autorizadas	Privilegios elevados para usuarios no administradores	Reducir	9 Control de Acceso
	E18.1	Pérdida parcial o total de información financiera	Falta de política de respaldos.	Reducir	12 Seguridad de Operación
	A8.1	Afectación por Malware	Falta de herramienta de protección corporativa.	Reducir	12 Seguridad de Operación
	E7.1	Información no actualizada	Deficiencia en controles y registro de mercaderías.	Reducir	8 Administración de Activo
	E4.1	Cambios sin control de parámetros del sistema por proveedores.	Falta de registro de control de cambios.	Reducir	14 Adquisición, desarrollo y mantenimiento del Sistema

4.4 Análisis de Selección de controles de seguridad.

En esta sección se muestra el consolidado de amenazas, vulnerabilidades, opciones de tratamiento, cláusulas de control de acuerdo al conteo realizado la mayoría de las opciones elegidas fueron reducir el riesgo, esto significa que el mayor esfuerzo depende de las mejoras internas aplicables a la infraestructura de tecnología y procedimientos necesarios para cubrir la operación y proteger los activos críticos, así como los controles seleccionados dentro de cada cláusula para ayudar con el objetivo de protección.

Tabla 16: Consolidado Opciones de Tratamiento. Fuente: Autor

Descripción	**Cantidad**
Total de Amenazas	43
Total de Vulnerabilidades	43
Opción de Tratamiento: Aceptar	7
Opción de Tratamiento: Reducir	35
Opción de Tratamiento: Transferir	1

Las cláusulas de control seleccionadas para reducir el riesgo son:

- ❖ Administración de Activos.
- ❖ Control de Acceso.
- ❖ Seguridad Física y Ambiental.
- ❖ Seguridad de Operaciones.
- ❖ Adquisición, Desarrollo y Mantenimiento del Sistema.

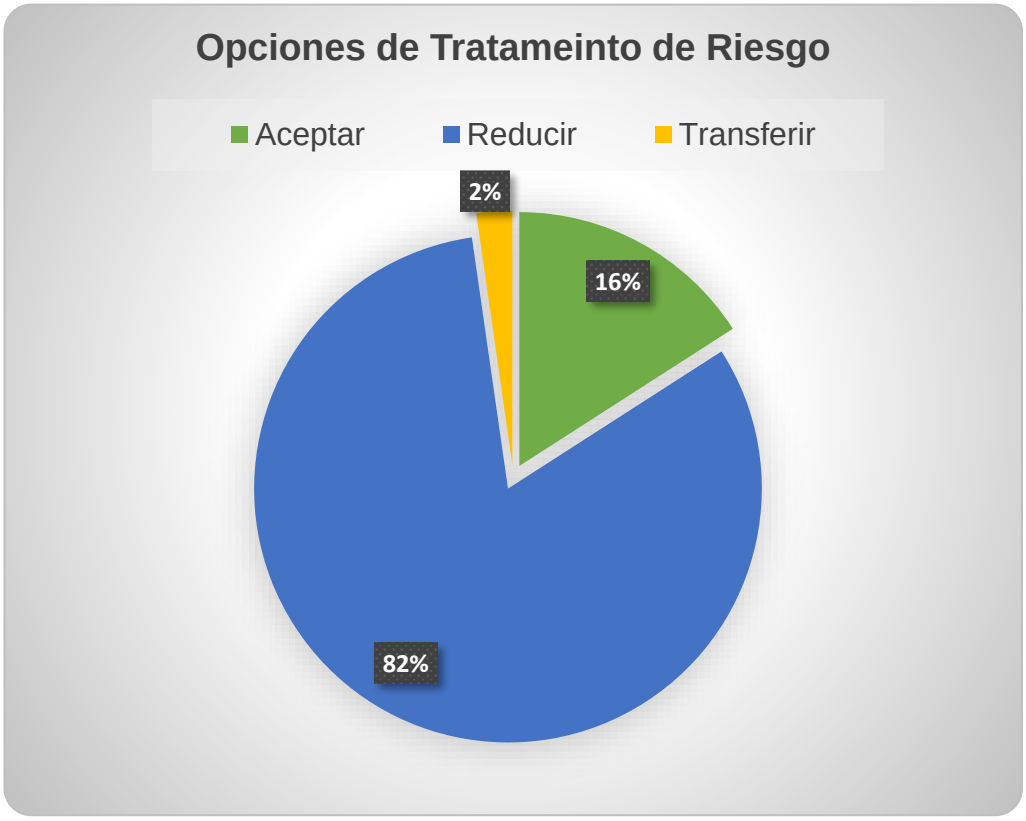


Figura 4.3 Opciones de Tratamiento. Fuente Autor

5 CAPÍTULO

DESARROLLO DE POLÍTICAS

5.1 Control: Cámara IP.

Tabla 17: Control de Cámara IP. Fuente: Autor

Activo de Información	Amenaza	Vulnerabilidad Relacionada	Opción de Tratamiento	Clausula de Seguridad	Control Seleccionado
Cámara IP	Fenómeno Natural	Exposición de cámaras sin protección.	Aceptar	N/A	N/A
	Errores de Mantenimiento	Falta de Mantenimiento Preventivo.	Reducir	11 Seguridad Física y Ambiental	11.2.4 Equipo y Mantenimiento
	Uso inadecuado	Dispositivo sin uso por falta de configuración.	Reducir	8 Administración de Activo	8.1.2 Propidad de Activo

5.2 Control: Dispositivo de Comunicaciones.

Tabla 18: Control Dispositivos de Comunicación. Fuente: Autor

Activo de Información	Amenaza	Vulnerabilidad Relacionada	Opción de Tratamiento	Clausula de Seguridad	Control Seleccionado
Dispositivo de Comunicación, Redes, Central IP	Indisponibilidad por interrupción de suministro eléctrico	No se tiene fuente redundante para estos equipos, posible daño en equipo.	Reducir	11 Seguridad Física y Ambiental	11.2 .2 Utilidades de Soporte
	Daño Lógico por Configuración	No se tiene respaldo de configuración.	Reducir	12 Seguridad de Operaciones	12.1.1 Procedimiento de Configuración Documentado. 12.5.1 Instalación de Sistemas Operacionales
	Daño Físico que requiere reemplazo total o parcial.	No existe contrato de mantenimiento con este tipo de Cobertura	Reducir	11 Seguridad Física y Ambiental	11.2.4 Mantenimiento de Equipo
	Degradación del servicio a causa de la internet	Solo se tiene un proveedor de internet.	Aceptar	N/A	N/A
	Uso inadecuado de equipos	Falta de conocimiento en la administración de la infraestructura.	Reducir	12 Seguridad de Operaciones	12.1.1 Procedimiento de Configuración Documentado 12.4.1 Registro y Seguimiento

5.3 Control: Servidor de Base de Datos

Tabla 19: Control de Base de Datos. Fuente: Autor

Activo de Información	Amenaza	Vulnerabilidad Relacionada	Opción de Tratamiento	Clausula de Seguridad	Control Seleccionado
Servidor de Base de Datos	Afectación por Malware	Falta de herramienta de protección corporativa	Reducir	12 Seguridad de Operaciones	12.2.1 Control Antimalware
	Pérdida parcial o total de información	No existe política de respaldo.	Reducir	12 Seguridad de Operaciones	12.3.1 Respaldo de Información
	Acceso a usuarios con claves débiles o por defecto.	No existe política de claves para usuarios a nivel de base de datos.	Reducir	9 Control de Acceso	9.2.3 Administración de privilegio y acceso. 9.4.3 Sistema de Administración de Clave
	Errores de Mantenimiento	Falta de procedimiento de parchado	Reducir	11 Seguridad Física y Ambiental	11.2.4 Mantenimiento de Equipos

5.4 Control: Dispositivos para usuario final

Tabla 20: Dispositivos para usuario final. Fuente: Autor

Activo de Información	Amenaza	Vulnerabilidad Relacionada	Opción de Tratamiento	Clausula de Seguridad	Control Seleccionado
Workstation/Portable, inventario/Activo, impresora.	Pérdida de Equipo	Ausencia de control y registro de inventarios	Reducir	8 Administración de Activo	8.1.2 Propietario de Activo
	Pérdida de información total o parcial	Falta de Respaldos para información sensible.	Reducir	12 Seguridad de Operaciones	12.3.1 Respaldo de Información
	Infección por Virus	Ausencia de Antivirus	Reducir	12 Seguridad de Operaciones	12.2.1 Control contra el Malware
	Secuestro de Información Ransomware	Falta de política de actualización y navegación.	Reducir	11 Seguridad Física y Ambiental	11.2.4 Mantenimiento de Equipos
	Listado de activo desactualizado o incompleto	Ausencia de política para manejo de activos	Reducir	8 Administración de Activo	8.2.3 Manejo de Activos
	Daño Físico de Activo	Lugar inapropiado de almacenaje.	Reducir	8 Administración de Activo	8.2.3 Manejo de Activos
	Acceso a través de credenciales por defecto.	Falta de política para usuarios de Administración	Reducir	9 Control de Acceso	9.2.3. Administraion de privilegio y acceso
	Errores de Mantenimiento	Falta de Mantenimiento Preventivo.	Reducir	11 Seguridad Física y Ambiental	11.2.4 Mantenimiento de Equipos
	Uso inadecuado de equipos	Poco conocimiento del dispositivo y su configuración.	Reducir	8 Administración de Activo	8.3.3 Transporte de Activos

5.5 Control: Dispositivos externos de Almacenamiento

Tabla 21: Control para Dispositivos externos. Fuente: Autor

Activo de Información	Amenaza	Vulnerabilidad Relacionada	Opción de Tratamiento	Clausula de Seguridad	Control Seleccionado
Dispositivos externos de almacenamiento	Fuga de Información	Ausencia de política por manejo de información en medios extraíbles.	Reducir	8 Administración de Activo	8.3.1 Gestión de Medios Extraibles
	Robo de Información	Ausencia de políticas por confidencialidad.	Aceptar	N/A	
	Infectación de malware	Ausencia de controles para revisión periódica de dispositivos externos.	Reducir	12 Seguridad de Operaciones	12.2.1 Control contra el Malware

5.6 Control de Activo: Persona

Tabla 22: Control Ejecutivo de Ventas y Logística. Fuente: Autor

Activo de Información	Amenaza	Vulnerabilidad Relacionada	Opción de Tratamiento	Clausula de Seguridad	Control Seleccionado
Ejecutivo de Ventas, Administrador de Bodega	Uso inadecuado de equipo/computador	Falta de control para correcto uso de dispositivo.	Reducir	8 Administración de Activo	8.1.2 Propiedad de Activos
	Robo de Información	Falta de controles sobre accesos y privilegios.	Reducir	9 Control de Acceso	9.1.1 Control de Acceso
	Indisponibilidad del Personal	Enfermedad	Aceptar	N/A	
	Divulgación de Información	Falta de Políticas de reserva y no divulgación.	Aceptar	N/A	
	Riesgo Interno	Uso excesivo de fuerza por manipulación de activo.	Aceptar	N/A	
	Daño Físico de Activo	Falta de conocimiento en manipulación.	Reducir	8 Administración de Activo	8.2.3 Manejo de Activos

5.7 Control: Servidor de Correo y Controlador de Dominio

Tabla 23: Control Servidor de Correo y Controlador. Fuente: Autor

Activo de Información	Amenaza	Vulnerabilidad Relacionada	Opción de Tratamiento	Clausula de Seguridad	Control Seleccionado
Servidor de Correo, Servidor Controlador de Dominio	Bloqueo parcial o total del servicio.	Afectación por SPAM.	Transferir	Contratar un servicio de protección especializado	N/A
	Suplantación de Identidad	Fraude por Pishing.	Reducir	12 Seguridad de Operaciones	12.2.1 Control Antimalware
	Robo de Información	Ataques de Ransomware	Reducir	11 Seguridad Física y Ambiental	11.2.4 Mantenimiento de Equipos. 12.6.1 Gestión de Vulnerabilidades.
	Indisponibilidad por interrupción de electricidad.	Falta de UPS.	Reducir	11 Seguridad Física y Ambiental	11.2.2 Herramientas de Apoyo.
	Errores de Mantenimiento	Falla en funcionamiento de activo	Reducir	11 Seguridad Física y Ambiental	11.2.4 Mantenimiento de Equipos
	Acceso físico y lógico sin control	Ausencia de políticas de acceso y uso.	Reducir	11 Seguridad Física y Ambiental	11.2.1 Localización y Protección de Equipos
	Errores de Mantenimiento	Falta de Mantenimiento	Reducir	11 Seguridad Física y Ambiental	11.2.4 Mantenimiento de Equipos
	Acceso no autorizado	Falta de Hardenización.	Aceptar	N/A	N/A

5.8 Control: Software de Ventas, Facturación, Inventario

Tabla 24: Control para Software varios. Fuente: Autor

Activo de Información	Amenaza	Vulnerabilidad Relacionada	Opción de Tratamiento	Clausula de Seguridad	Control Seleccionado
Software de Ventas, Software de Inventario, Software de Facturación.	Fuga de Información	Falta de control por acceso a la información.	Reducir	9 Control de Acceso	9.1.1 Control de Acceso
	Operaciones no autorizadas	Privilegios elevados para usuarios no administradores	Reducir	9 Control de Acceso	9.2.3 Administración de privilegio de acceso
	Pérdida parcial o total de información financiera	Falta de política de respaldos.	Reducir	12 Seguridad de Operaciones	12.3.1 Respaldo de Información
	Afectación por Malware	Falta de herramienta de protección corporativa.	Reducir	12 Seguridad de Operaciones	12.2.1 Control Antimalware
	Información no actualizada	Deficiencia en controles y registro de mercaderías.	Reducir	8 Administración de Activo	8.1.2 Propiedad de Activo
	Cambios sin control de parámetros del sistema por proveedores.	Falta de registro de control de cambios.	Reducir	14 Adquisición, desarrollo y mantenimiento del Sistema	14.2.2 Procedimiento de Control para Cambios del Sistema

5.9 Diseño de Políticas para Seguridad de la Información.

Las políticas están realizadas para poder brindar un nivel de protección a un determinado activo expuesto a determinadas amenazas y que pueden explotar una o más vulnerabilidades asociadas a un activo, la solución está basada en el análisis de riesgo de capitulo anterior y se detalla a continuación:

5.10 Cláusula de Administración de Activo

- Registrar los activos de información de forma oportuna, con los campos y características requeridos.
- Definir un flujo de autorizaciones para el acceso al activo de acuerdo al nivel de criticidad del mismo.
- El inventario debe ser controlado y validado de forma periódica de tal manera que este actualizado.
- El activo debe ser almacenado de acuerdo a las condiciones y recomendaciones descrita por fábrica para que se mantenga integro.
- El transporte o movilización del activo debe ser realizado por personal de confianza y autorizado por la compañía.
- El personal interno o externo que traslade un activo debe tener identificación para entrega/ recepción de activo.
- El activo debe ser trasladado con protección de tal forma que garantice la integridad del mismo ante la humedad, calor, golpe.

- El acceso a medios extraíbles debe ser habilitado únicamente si existiera la necesidad de uso.
- El medio extraíble con información crítica debe ser almacenado en un entorno seguro para salvaguardar la integridad del medio y la información que reside dentro.
- Si alguna información crítica almacenada en un medio extraíble no será utilizada en ningún otro momento, entonces, se debe proceder con la eliminación segura de la información para garantizar que alguien no autorizado no logre obtenerla.

5.11 Cláusula de Control de Acceso

- El nivel de privilegio asociado a cada usuario para un sistema operativo o aplicación debe ser analizado y autorizado basado en la necesidad y responsabilidad del usuario solicitante.
- El nivel de privilegio solicitado por un usuario no debe ser aplicado por personal de tecnología hasta que la solicitud no esté autorizada por el ente correspondiente.
- Los niveles de privilegios altos o especiales, deben ser asignados a usuarios diferentes a los usuarios ya existente para la ejecución de tareas diarias y los usuarios con alto nivel de privilegio no deben ser utilizados para la ejecución de tareas de operación.
- El uso de usuarios genéricos que vienen embebidos en configuraciones de fábrica deben ser protegidos para que mantengan

su confidencialidad ante cualquier situación de exposición ya sea por cambios en la administración o por rotación de personal.

- Las credenciales para distintos ambientes deben ser segmentadas de tal forma que se pueda tener mayor control y trazabilidad.
- Las contraseñas seleccionadas deben cumplir con el uso de mayúsculas, minúsculas, símbolos especiales y números con una longitud de 8 a 12 caracteres.
- Los usuarios nuevos deben ser obligados a cambiar la contraseña de forma automática después del primer logon.
- La contraseña debe cumplir con el tiempo de expiración de 45 días, luego de eso se debe cambiar la contraseña de forma obligatoria.
- No se puede utilizar las últimas tres contraseñas.
- La contraseña no puede ser visible al momento de ingresarla.
- Debe existir concordancia entre los accesos de un usuario y la política de información para sistemas y redes.
- El permiso requerido por un usuario no debe contradecir las políticas establecidas para protección de activos.
- Los roles para un usuario deben ser establecidos de acuerdo al control de acceso autorizado.
- Se deben realizar revisiones una vez al año para validar que los niveles de acceso otorgados a un usuario deban mantenerse de acuerdo a las funciones y responsabilidades del solicitante.

5.12 Cláusula de Seguridad Física y Ambiental

- Se debe realizar mantenimiento físico y lógico a los activos físicos y los que son intangibles como base de datos, aplicaciones, sistemas operativos, etc.
- La frecuencia del mantenimiento debe realizarse de acuerdo a lo recomendado por fábrica, para los activos que apliquen el mantenimiento debe ejecutarse al menos una vez al año.
- El mantenimiento debe ser ejecutado por personal capacitado y autorizado.
- Los mantenimientos ya sean correctivos o preventivos deben ser registrados en bitácora para posterior control.
- Antes de colocar el activo de retorno a la operación posterior al mantenimiento se debe realizar una revisión para asegurarnos que está funcionando de forma correcta.
- Los equipos deben ser mantenidos de acuerdo a lo especificado por fábrica con la finalidad de mantenerlo de forma óptima.
- Para los equipos de tecnología que cumplen con funciones específicas de forma exclusiva se debe considerar tener una fuente redundante y una toma de electricidad adicional de distinto origen.
- Los equipos deben ser ubicados de tal manera que minimicen el acceso necesario a las instalaciones donde se encuentran.

- Los componentes de los activos que requieren protección especial deben ser almacenados para reducir el nivel de exposición y riesgo asociado.
- Está prohibido alimentarse, tomar algún tipo de bebida, así como fumar dentro o cerca de las instalaciones de computo.
- Las instalaciones donde se encuentran los equipos de tecnología deben estar en temperaturas recomendadas por fábrica.

5.13 Cláusula de Seguridad de Operaciones

- Los procedimientos de configuración de un sistema operacional, herramienta o aplicación deben ser almacenados y mantenidos como histórico.
- Los niveles de escalamiento para manejos de incidentes, reporte de novedades y requerimientos debe estar actualizado y accesible para los responsables y administradores de los activos.
- Tener acceso a los procedimientos documentados con primeros pasos a seguir ante fallos del sistema operativo del activo y demás componentes.
- Se debe tener un procedimiento de reverso en caso que la ejecución de un procedimiento operacional por configuración o actualización no funcione de acuerdo a lo esperado.

- En caso de las actualizaciones, las versiones previas deben se almacenadas como medida de contingencia durante el proceso de actualización.
- Logs de las plataformas y sistemas críticos deben ser revisados de forma periódica con el objetivo de detectar cualquier funcionamiento fuera de lo común.
- Logs por cambios en la configuración deben ser almacenados para revisiones posteriores según sea requerido por personal de tecnología.
- Está prohibido la instalación y uso de software no autorizado por la administración.
- La persona responsable de tecnología debe revisar trimestralmente las vulnerabilidades asociadas a los activos de información, evaluar el riesgo, seguimiento a parchado de activos, rastreo de activos, etc.
- En caso de detectar una vulnerabilidad potencialmente técnica se debe tomar una acción en los próximos tres días laborales.
- Dependiendo en la urgencia de la remediación de la vulnerabilidad debe ser tratada de acuerdo a los controles de gestión de cambio o manejarlo como un incidente de seguridad de la información.
- Se debe definir un procedimiento ante la situación donde una vulnerabilidad ha sido identificada pero no existe opciones de remediación. Para este caso el responsable de tecnología debe

evaluar el riesgo de la vulnerabilidad y definir acciones de soporte para detección y corrección en 10 días.

- Se debe reducir de forma prioritaria las vulnerabilidades con criticidad alta y medianas asociados a activos críticos que pueden ser explotadas por algún tipo de malware.
- Se debe utilizar herramienta de apoyo con administración centralizada para protección y detección de malware.
- Es responsabilidad de personal de tecnología revisar la información relacionada a los hallazgos de nuevo malware a través de publicaciones de sitio conocidos mediante boletines.
- Los respaldos de información deben realizarse sobre las bases de datos que alojan información del negocio, así como demás herramientas de apoyo a la administración.
- La frecuencia de los respaldos dependerá de la criticidad de la información a respaldar y del tiempo necesario para que el respaldo se logre ejecutar sin afectar el rendimiento. Las bases de datos se deben respaldar mínimo de manera semanal.
- El monitoreo por ejecución de los respaldos debe ser realizado de acuerdo a la frecuencia de los respaldos con la finalidad que todos los programados se logren completar de forma exitosa, en caso de detectar error en alguna tarea se debe relanzar la tarea de respaldo.

- Los respaldos deben ser almacenados en ubicaciones remotas, lo suficientemente distantes para escapar de cualquier daño en Matriz.
- Los respaldos deben ser probados de forma regular para validar el procedimiento de recuperación y tener un tiempo estimado de recuperación en caso que amerite hacerlo en producción. Este ejercicio debe ser realizado en un ambiente controlado de prueba para evitar el riesgo de afectar el ambiente productivo. La frecuencia de este ejercicio debe ser al menos una vez al año y debe existir bitácora de las bases probadas, así como del resultado de la prueba.

5.14 Cláusula para la Adquisición, Mantenimiento y Desarrollo de Sistemas.

- Los cambios realizados en los sistemas a nivel lógico deben tener la autorización de administración previa ejecución.
- Identificar todos los componentes lógicos que requieren modificación.
- Identificar y revisar codificaciones críticas a nivel de seguridad para evitar puntos de fallo o vulnerabilidades a nivel de software.
- Asegurarnos que los usuarios autorizados son quienes reciben el cambio.
- Asegurarnos que la documentación del sistema este actualizada de acuerdo a cada cambio realizado y que la documentación anterior quede como histórico o sea eliminado si se deseara.

- Se debe mantener un control de versión por cada actualización de software.
- Se debe garantizar que el cambio realizado sea ejecutado en el tiempo correcto y no genere molestias para usuarios del negocio.

5.15 Aplicación de buenas prácticas de seguridad

A continuación, se muestra el consolidado de las políticas seleccionadas, un total de 62 políticas correspondientes a 5 dominios, versus el número de controles existentes de la norma ISO 27002 que corresponde a un total de 114 controles, en el mismo se puede apreciar los dominios con mayor cobertura y aquellos que no forman parte del alcance.

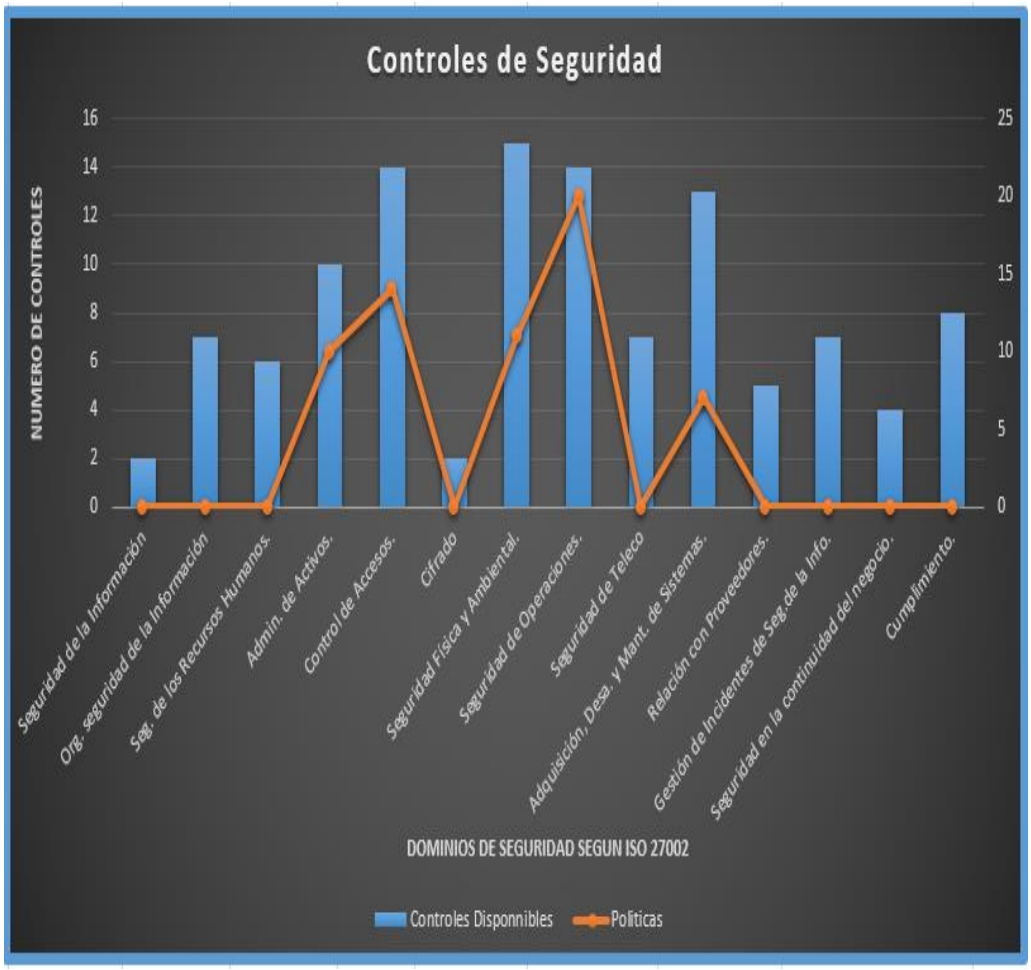


Figura 5.1 Consolidado de Controles y Políticas. Fuente: Autor

6 CAPÍTULO

ANÁLISIS DE RESULTADOS

Con el objetivo de garantizar el cumplimiento de las políticas establecidas para cada sección o categoría y conocer si la solución propuesta a nivel de control cumple con los objetivos de la compañía, se debe evaluar las políticas establecidas posterior a un periodo de implementación asegurándonos que el ambiente se encuentra estable, Los criterios sugeridos de evaluación son: forma de aplicación, efectos post implementación, disminución de incidentes o problemas.

6.1 Revisión de los riesgos mitigados

Tabla 25: Revisión de Riesgos Mitigados. Fuente: Autor

Activo	Valor Activo	No.	Amenaza	Vulnerabilidad	Probabilidad	Riesgo
Software de Ventas	4,33	1	Malware	Falta de protección antimalware.	3	8,66
		2	Fuga de Información	Falta de control por acceso a la información.	3	8,66
		3	Operaciones no autorizadas	Privilegios elevados para usuarios no administradores	4	4,33
		4	Pérdida parcial o total de información financiera	Falta de política de respaldos.	3	8,66
Workstation/ Portable	3,66	5	Pérdida de Equipo	Ausencia de control y registro de inventarios	3	3,66
		6	Pérdida de información total	Falta de Respaldos para información sensible.	4	3,66
		7	Infección por Virus	Ausencia de Antivirus	4	7,32
		8	Secuestro de información Ransomware	Falta de política de actualización y navegación.	1	3,66
Dispositivos de Comunicación	4,33	9	Indisponibilidad por corte de energía	No se tiene fuente redundante para estos equipos.	3	4,33
		10	Daño Lógico por Configuración	No se tiene respaldo de configuración.	2	4,33

		11	Daño Físico que requiere reemplazo total o parcial	No existe contrato de mantenimiento con este tipo de Cobertura	2	8,66
Ejecutivo de Ventas	4,33	12	Mal uso de Activo	Falta de control y uso por desconocimiento. de activo.	3	4,33
		13	Hurto de Información	Falta de controles sobre accesos y privilegios.	3	4,33
		14	Indisponibilidad del Personal	Enfermedad	3	8,66
		15	Divulgación de Información	Falta de Políticas de reserva y no divulgación.	3	8,66
Central IP	4,33	16	Daño de central por inconvenientes de energía	Conexión de energía directas sin protección contra variaciones.	2	4,33
		17	Degradación del servicio a causa de la internet	Solo se tiene un proveedor de internet.	2	4,33
Servidor de Correo	4,66	18	Bloqueo parcial o total del servicio.	Afectación por SPAM.	4	9,32
		19	Suplantación de Identidad	Fraude por Pishing.	1	4,66
		20	Afectación por Malware	Infección de virus por falta de protección.	3	4,66
		21	Secuestro de Información	Ataques de Ransomware	1	4,66
		22	Propagación de infección a través del servicio	Infección por archivos adjuntos.	4	9,32
		23	Acceso no autorizado local.	Falta de Hardenización.	3	4,66

		24	Acceso remoto no autorizado	Seguridad de conexión remota, débil o inexistente.	3	9,32
Sistema de Inventario	4,33	25	Afectación por Malware	Falta de herramienta de protección corporativa.	3	4,33
		26	Información no actualizada	Deficiencia en controles y registro de mercaderías.	4	8,66
		27	Activos categorizados de forma incorrecta	Deficiente administración de activos.	4	4,33
		28	Pérdida parcial o total de información.	No existe política de respaldos.	3	4,33
Sistemas de Facturación	4,66	29	Afectación por Malware	Falta de herramienta de protección corporativa	3	4,66
		30	Pérdida parcial o total de información.	No existe políticas de respaldo.	3	4,66
		31	Cambios sin control de parámetros del sistema por proveedores	Falta de registro de control de cambios.	4	
Servidor de Base de Datos	4,66	32	Afectación por Malware	Falta de herramienta de protección corporativa	3	4,66
		33	Pérdida parcial o total de información	No existe política de respaldo.	3	4,66
		34	Afectación al motor de base de datos	No existe proceso de parchado para motor.	4	9,32
		35	No hay control para acceso de usuarios de aplicativos	No existe política de claves para usuarios a nivel de base de datos ni aplicativos	3	9,32

Servidor Controlador de Dominio	4,66	36	Componentes y servicios desactualizados	Falta de procedimiento de parchado para servidor.	4	4,66
		37	Afectación por Malware	Falta de herramienta de protección corporativa	3	4,66
		38	Método de recuperación ante fallos	No existe documentación de la instalación	3	9,32
		39	Acceso físico y lógico sin control	Ausencia de políticas de acceso y uso.	3	9,32
		40	Daño físico o lógico	Falta de mantenimiento y revisiones periódicas.	4	9,32
		41	Servicios no autorizados	Falta de Hardenización.	4	4,66
Cámara IP	3	42	Fenómeno Natural	Exposición de cámaras sin protección.	1	3
		43	Inoperatividad de dispositivos	Falta de Mantenimiento y revisiones periódicas.	3	3
		44	Inoperatividad parcial o total	Funciones sin uso por mala configuración.	4	3
Inventario/ Activo	4	45	Listado de activo desactualizado o incompleto	Ausencia de política para manejo de activos	4	8
		46	Daños Físico de Activo	Lugar inapropiado de almacenaje.	3	4
		47	Pérdida de Activo	Deficiente administración de Activo	2	4

Impresora	1,66	48	Acceso a través de credenciales por defecto.	Falta de política para usuarios de administración.	4	3,32
		49	Inoperatividad de dispositivos.	Falta de Mantenimiento Preventivo.	3	1,66
		50	Uso de servicios no autorizados	Poco conocimiento del dispositivo.	3	1,66
Administrador de Bodega	4,33	51	Riesgo Interno	Uso excesivo de fuerza por manipulación de activo.	3	4,33
		52	Indisponibilidad del personal	Enfermedad o Calamidad Domestica	4	4,33
		53	Daño parcial de activo	Falta de conocimiento en manipulación de equipos	3	4,33
Dispositivos externos de almacenamiento	3,66	54	Fuga de Información	Ausencia de política por manejo de información en medios extraíbles	3	3,66
		55	Robo de Información	Ausencia de políticas por confidencialidad.	2	3,66
		56	Infectación de malware	Ausencia de controles para revisión periódica de dispositivos externos.	4	3,66

6.2 Análisis de resultado posterior a los controles

Los resultados de la implementación de los controles se pueden apreciar con el ejercicio del cálculo de riesgo realizado en la sección anterior, para mejor comprensión se realiza un mapa de calor con el impacto estimado posterior a las políticas aplicadas.

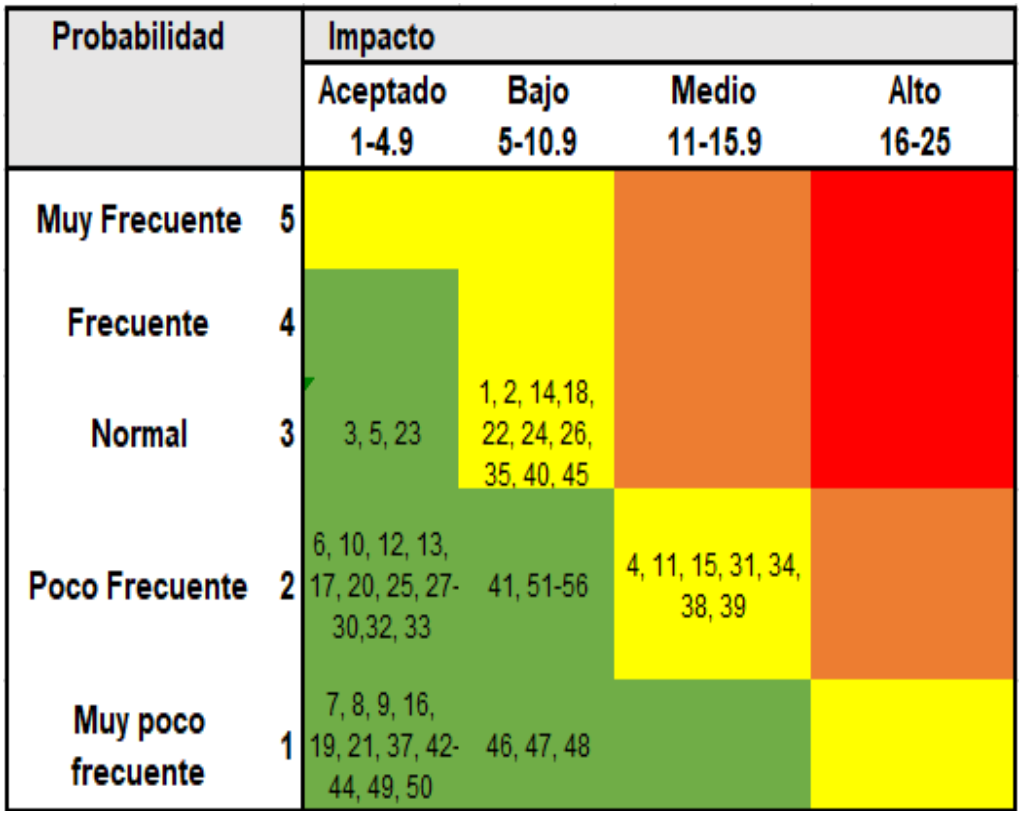


Figura 6.1 Mapa de Calor de Riesgo posterior a políticas. Fuente: Autor

CONCLUSIONES Y RECOMENDACIONES

1. Conclusiones

1.1 Se concluye que el conjunto de controles y políticas aplicadas logra disminuir considerablemente el nivel de riesgo sobre activos críticos de información, y ofrece una visión holística sobre el posible impacto en caso que una amenaza se materialice.

1.2 Se evidencia que las tareas del equipo de tecnología se han enfocado principalmente en la parte funcional y no se ha considerado recomendaciones de seguridad para protección de información en la capa lógica o física.

1.3 La solución implementada ofrece un nivel de protección, pero no garantiza la cobertura total para mantener la disponibilidad de un servicio en particular.

1.4 Las tareas de remediación de vulnerabilidades no representan un alcance de un proyecto ya que son frecuentes y su nivel de criticidad cambia en el tiempo de forma inherente a las tecnologías y plataformas utilizadas.

1.5 La correcta organización y documentación de procedimientos disminuirá la cantidad de incidentes por errores no intencionales y evitará la dependencia de un único especialista ya que la información esta socializada y compartida.

1.6 El trabajo realizado me ayudó a la compresión de forma responsable sobre la preparación continua que se debe tener para poder enfrentar situaciones de alto riesgo y mantenerse a la vanguardia sobre el uso de herramientas y amenazas existentes, así como la importancia de socializar con todo el equipo de trabajo las directrices que ayudarán a cumplir con los objetivos de control.

2. Recomendaciones

2.1 La seguridad de la información debe ser practicada de forma continua por cada miembro de la organización, hasta que se convierta en cultura organizacional.

2.2 Los componentes de infraestructura de tecnología tienen habilitadas las funciones predeterminadas de fábrica, se recomienda aprovechar características de dichas herramientas para el apoyo en relación a protección del activo de información.

2.3 Conocer el correcto funcionamiento de los componentes de la plataforma por parte del equipo de tecnología y responsables de seguridad ayuda a mantener y mejorar el rendimiento del activo, así como la toma de decisiones y resolución de incidentes en menor tiempo.

2.4 La capacitación de forma continua prepara y compromete al personal responsable a responder ante cualquier evento que exponga la disponibilidad de algún servicio.

BIBLIOGRAFÍA

[1] ISOTools Excellence, Vulnerabilidades de la organización por ISO Tools Excellence, https://www.pmg-ssi.com/2015/06/iso-27001-vulnerabilidades-de-la-organizacion/.Junio 2015.

[2] Ministerio de Hacienda y Administraciones Públicas – Gobierno de España. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1 – Método. Página 9.

[3] ISOTools Excellence, Plan de Tratamiento de riesgos de seguridad de la información, https://www.pmg-ssi.com/2017/05/iso-27001-plan-de-tratamiento-de-riesgos-de-seguridad-de-la-informacion/ Mayo 2017.

[4] [5] [6] Ministerio de Hacienda y Administración Públicas, Magerit-Versión 3.0 Metodología de Análisis y Gestión de Riesgo de los Sistemas de Información; https://edoc.site/magerit-v3-completo-pdf-free.html; Madrid, Octubre del 2012.

[7] ISO Tools Excellence, 4 Opciones de mitigación en el tratamiento de riesgo según ISO 27001; https://www.isotools.org/2017/08/20/4-opciones-mitigacion-tratamiento-riesgos-segun-iso-27001/. Agosto 2017.

[8] ISO ORG, ISO/IEC 27002:2013 Information Technology - Security techniques – Code of practice for information security controls. Octubre 2013.

[9] Instituto Nacional de Ciberseguridad de España, Amenaza vs. Vulnerabilidad;https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian. Marzo 2017.

[10] Ministerio de Hacienda y Administraciones Públicas – Gobierno de España. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1 – Método. Página 7.

[11] Ministerio de Hacienda y Administraciones Públicas – Gobierno de España. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1 – Método. Página 50-53.