ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE SISTEMAS

PROYECTO INTEGRADOR DE INVESTIGACIÓN Y DESARROLLO

PROPUESTA DE UN CICLO DE GESTIÓN DE RIESGOS UTILIZANDO MODELOS DE AMENAZAS Y CONTROLES DE SEGURIDAD ISO/EC 27002 / EGSI / RGPD

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL GRADO DE MAGISTER EN SOFTWARE

RICARDO ALCIBIADIS PERUGACHI CARTAGENA
ricardo.perugachi@epn.edu.ec

Director: Denys Alberto Flores Armas
denys.flores@epn.edu.ec

2020

APROBACIÓN DEL DIRECTOR

Como director del trabajo de titulación “Propuesta de un ciclo de gestión de riesgos utilizando modelos de amenazas y controles de seguridad ISO/EC 27002/EGSI/RGPD” desarrollado por Ricardo Alcibiadis Perugachi Cartagena, estudiante de la Maestría en Software, habiendo supervisado la realización de este trabajo y realizado las correcciones correspondientes, doy por aprobada la redacción final del documento escrito para que prosiga con los trámites correspondientes a la sustentación de la Defensa oral.

Digitally signed by DENYS ALBERTO FLORES ARMAS
DN: cn=DENYS ALBERTO FLORES ARMAS, serialNumber=231120155658, ou=ENTIDAD DE CERTIFICACION DE INFORMACION, o=SECURITY DATA S.A. 2, c=EC
Date: 2021.02.02 19:52:36 -05'00'

Denys Alberto Flores Armas MSc.

DIRECTOR

DECLARACIÓN DE AUTORÍA

Yo, Ricardo Alcibiadis Perugachi Cartagena, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Ricardo Alcibiadis Perugachi Cartagena

DEDICATORIA

Dedico el presente trabajo de tesis a mi amada esposa Paulina quien, con su apoyo y amor incondicionales, ha sido esa roca fuerte que día a día me ha impulsado a alcanzar todas las metas que me he propuesto tanto en el aspecto profesional, académico y personal. Sin tu presencia en mi vida, nada sería igual y nada tendría el valor que tiene. Gracias por iluminar mis días con tu paciencia y amor. Por esto y muchos motivos más, este trabajo es para ti mi vida.

AGRADECIMIENTO

En primer lugar, quiero agradecer a Dios por todas las bendiciones recibidas, pues toda actividad emprendida debe tener como centro al Todopoderoso.

Agradezco a mi familia, mi madre, esposa e hijos quienes con su presencia diaria me han impulsado a alcanzar una nueva meta.

Agradezco a la Escuela Politécnica Nacional, ese centro del saber que me ha acogido para permitirme adquirir nuevos y valiosos conocimientos.

Finalmente agradezco a mi tutor, quien con su experiencia y conocimiento me ha guiado en el proceso de este trabajo que me ha enriquecido en el aspecto académico y profesional.

ÍNDICE DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

RESUMEN

En la actualidad una mayor cantidad de sistemas de información consumen y almacenan datos sensibles de sus distintos actores, considerando que la información es un activo valioso, cada día se presentan más ataques que tratan de robar estos datos, vulnerando así no solo los sistemas, sino también la privacidad de las personas. Frente a esta realidad es necesario realizar una gestión de riesgos adecuada, que considere la privacidad de la información y que permitan a las organizaciones proteger los datos sensibles que poseen.
Esta tesis de Maestría tiene como objetivo proponer un "Ciclo de Gestión de Riesgos", que haga uso de los lineamientos provistos por el estándar ISO 27005, tomando en cuenta los controles propuestos por la norma internacional ISO 27002, así como también los lineamientos de el "Esquema Gubernamental de Seguridad de la Información" del estado ecuatoriano y finalmente considerando el "Reglamento General de Protección de Datos" europeo con el propósito de asegurar la privacidad de los datos personales sensibles.
El ciclo de gestión de riesgos a proponer será evaluado mediante un caso de estudio basado en distintos ataques a la información sensible reportados en la red, una vez definido el caso de estudio se procederá a realizar un modelo automatizado de amenazas y para la evaluación de riesgos se utilizarán árboles de ataque y defensa. Durante el ciclo de gestión de riesgos se trabajará tanto con el riesgo inherente como con el riesgo residual, que son los valores que determinarán que tan efectivo ha sido el ciclo.
Se pretende que el presente trabajo sea un aporte valioso para que las empresas puedan realizar la gestión de riesgos con el uso de herramientas automatizadas que faciliten análisis cualitativos y cuantitativos.

Palabras clave: Ciclo de Gestión de Riesgos. Esquema Gubernamental de Seguridad de la Información. Reglamento General de Protección de Datos. Árboles de ataque y defensa.

ABSTRACT

At present, a greater number of information systems consume and store sensitive data of their different actors, considering that information is a valuable asset, every day there are more attacks that try to steal this data, thus violating not only the systems, but also also the privacy of people. Faced with this reality, it is necessary to carry out adequate risk management, which considers the privacy of the information and allows organizations to protect the sensitive data they possess.

The objective of this Master's thesis is to propose a "Risk Management Cycle", which makes use of the guidelines provided by the ISO 27005 standard, taking into consideration the controls proposed by the international standard ISO 27002, as well as the guidelines of the "Government Information Security Scheme" of the Ecuadorian state and finally considering the European "General Data Protection Regulation" in order to ensure the privacy of sensitive personal data.

The risk management cycle to be proposed will be evaluated through a case study based on different attacks on sensitive information reported in the network, once the study is defined, an automated threat model will be carried out and risk assessment will be carried out they will use attack and defense trees. During the risk management cycle, work will be done with both inherent risk and residual risk, which are the values that will determine how effective the cycle has been.

This work is intended to be a valuable support so that companies can carry out risk management with the use of automated tools that facilitate qualitative and quantitative analysis.

Keywords: Risk Management Cycle. Government Information Security Scheme. General Data Protection Regulation. Trees of attack and defense.

1. INTRODUCCIÓN

En el mundo actual las empresas tanto públicas como privadas manejan una mayor cantidad de información, sea esta propia o de terceros, estos datos pueden incluir o no datos sensibles, este incremento de información está enfocado en mejorar la competitividad, ayudando a las empresas a entregar de manera más eficiente y eficaz sus distintos servicios o productos [1]. Sin embargo, junto al incremento de prestaciones, también aumentan los riesgos a los que la información se encuentra expuesta, y no solo eso, pues también la privacidad de los propietarios originales de la información se ve expuesta. Si se tiene presente que "La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización" [2], se hace manifiesto que la gestión de la seguridad de la información es de fundamental importancia en las compañías

1.1. Planteamiento del problema

Los ataques que buscan filtrar y aprovechar información confidencial son más comunes y van en aumento día a día, en Ecuador por ejemplo en el mes de abril del año 2019 se detectaron alrededor de 40 millones de ataques por parte de piratas informáticos a varias entidades estatales [3]. En Ecuador la firma de seguridad VPN Mentor detectó la sustracción de una base de datos ecuatoriana, con información de más de 20 millones de personas [4], Por este motivo, es indispensable asegurar la información de manera tal que se pueda garantizar la continuidad de las operaciones de las organizaciones, así como la privacidad de sus clientes y usuarios.

Para permitir a las empresas manejar los peligros a los que se encuentran expuestas, actualmente se da una importancia creciente y protagónica a la gestión de los riesgos. Debido a la evolución del contexto socioeconómico, las organizaciones están sometidas a factores de riesgo cada vez más lejanos a su entorno próximo, con frecuencia atípicos o singulares, y cuyo tratamiento no depende únicamente de decisiones rápidas, sino de estrategias preventivas especializadas. Por este motivo, se hace necesario el desarrollo de mecanismos de control interno sustentados principalmente en los sistemas de información, así como la implantación de estrategias destinadas a identificar los diferentes factores de riesgo y el valor económico que podría afectar a la empresa si esos riesgos se materializan, se necesita también el diseño de políticas destinadas a minimizar dichos riesgos. El aplicar una correcta gestión de riesgos puede contribuir al progreso de las

empresas mejorando la calidad y confiabilidad de los procesos internos, e incrementando las oportunidades de supervivencia de estas, su planteamiento proporciona un esquema muy concreto de los factores de exposición que afectan a cualquier organización [5].

El Estándar ISO 27005 proporciona pautas para la gestión de riesgos de seguridad de la información. Gran parte del lenguaje utilizado en este estándar es común y se basa en los siguientes componentes clave del proceso de gestión de riesgos. El primer paso es el "establecimiento de contexto" que implica definir cómo llevar a cabo la gestión de riesgos, escribir procedimientos y alinearlos con las agendas corporativas. El siguiente paso es “realizar una evaluación de riesgos” para identificar riesgos potenciales y sus posibles impactos, antes de construir un “tratamiento de riesgo”, que implica resolver el que hacer con ellos. Finalmente debe establecerse “una manera formal y estructurada de recopilar datos y registrarlos e informar sobre los resultados de la gestión” [6].

Una parte fundamental de la gestión de riesgos es la selección e implementación de controles de seguridad tanto para sistemas de información como para las empresas, dichos controles pueden tener implicaciones importantes en las operaciones y activos de las organizaciones, así como en el bienestar de las personas. Los controles de seguridad son las salvaguardas o contramedidas prescritas para los sistemas de información u organizaciones que están diseñados para: proteger la confidencialidad, integridad y disponibilidad de la información que es procesada, almacenada y transmitida por dichos sistemas u organizaciones, y satisfacer un conjunto definido de requerimientos de seguridad [7].

En el ámbito ecuatoriano las instituciones del sector público definen sus controles de seguridad a través del “Esquema Gubernamental de Seguridad de la Información” (EGSI) el cual es un esquema de seguridad basado en la norma ISO/IEC 27002, mismo que es utilizado por las diversas entidades de la administración pública central [8]. En cuanto a la accesibilidad de la información, en el Ecuador existe la ley orgánica de transparencia y acceso a la información pública (LOTAIP), que garantiza a los ciudadanos y a cualquier interesado acceder a la información de las entidades públicas cumpliendo determinados parámetros, Por otro lado, tenemos que a nivel país debido a la filtración de información de la que fue objeto la mayoría de la población del país [4], dio pie a que la Presidencia de la República, a través del Ministerio de Telecomunicaciones, anuncie que remitirá al órgano legislativo un Proyecto de Ley Orgánica de Protección de Datos Personales (LOPD), sobre el cual la Dirección Nacional de Registro de Datos Públicos (DINARDAP) ha estado trabajando por más de tres años. En ese sentido, a través de la mencionada ley se pretende proteger la información de carácter personal que por cualquier motivo se deba compartir para tener acceso a ciertos productos o servicios. Al continuar este marco

legal como proyecto hoy en día, se vuelve necesario buscar otro reglamento para normalizar la privacidad de los datos, por este motivo, saliendo del ámbito nacional, en Europa se implementó en el año 2016 el "Reglamento General de Protección de Datos" (RGPD) mismo que tiene gran inferencia a nivel mundial y hoy en día más países utilizan este reglamento como punto de referencia para el correcto manejo de la privacidad de sus datos [9].

1.2. Pregunta de investigación

En base al problema planteado surge la pregunta de investigación.

¿Es viable implementar un ciclo de gestión de riesgos que integre el uso de controles de seguridad ISO/IEC 27002, usando el Esquema Gubernamental de Seguridad de la Información y el Reglamento General de Protección de Datos, para considerar la privacidad de los datos personales sensibles?

1.3. Objetivo general

Proponer un ciclo de gestión de riesgos utilizando modelos de amenazas y controles de seguridad ISO/IEC 27002/EGSI / RGPD.

1.4. Objetivos específicos

Derivados del objetivo general se proponen los siguientes objetivos específicos:

- Identificar mediante un estudio sistemático de literatura un escenario de ataque que considere las amenazas más comunes a la seguridad y privacidad de información.
- Evaluar el riesgo inherente y residual en el escenario propuesto, usando árboles de ataque y defensa
- Diseñar un procedimiento que facilite la gestión de riesgos, integrando ISO 27002/EGSI, ISO 27005 y RGPD
- Documentar una guía simple para su implementación.

1.5. Marco Teórico

Un primer paso para comprender la necesidad de seguridad sobre la información consiste en entender sus distintas dimensiones:

Disponibilidad: disposición de los servicios a ser usados cuando sea necesario [10].

Integridad: característica que hace referencia de completitud y corrección de los datos [10].

Confidencialidad: indica que la información llegue solamente a las personas autorizadas [10].

A estas dimensiones canónicas de la seguridad se pueden añadir otras derivadas que están relacionadas con la percepción de los usuarios de los sistemas de información:

Privacidad: es la propiedad o característica que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros [10].

Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos [10].

Trazabilidad: aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento [10].

Todas estas características pueden ser requeridas o no dependiendo de cada caso y organización. Cuando son necesarias, estás no están presentes sin antes poner de por medio un esfuerzo para conseguirlas. A racionalizar este esfuerzo se dedica el análisis y la gestión de riesgos, en este contexto se tiene que:

Vulnerabilidad: es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de esta, por lo que es necesario encontrarlas y eliminarlas lo antes posible [10].

Amenaza: es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas [10].

Riesgo: es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro [10].

El riesgo por sí solo es simplemente un número. Una medida de riesgo solo tiene sentido cuando se compara con otra medida de riesgo. Decir que algo es "demasiado arriesgado" implica que el riesgo en cuestión excede algún otro nivel de riesgo aceptable. Decir "es seguro" significa que no. El riesgo es una medida relativa. ¿Qué es aceptable para una organización? Además, esa medida de riesgo en sí misma solo tiene sentido para un sistema y una organización en particular. Robert Courtney Jr., de IBM, resumió esto en su primera ley: "No se puede decir nada interesante (es decir, significativo) acerca de la seguridad de un sistema, excepto en el contexto de una aplicación y entorno particulares". ¿Dónde está el contexto que miramos al examinar el riesgo? Podemos mirar directamente a las propias organizaciones [11].

Los profesionales de seguridad de TI tienen una definición específica de riesgo: el evento en el que algo malo le sucede a algo que nos importa. El riesgo se compone de dos subcomponentes: probabilidad (oportunidad) e impacto (algo malo). Decir: "Si esta máquina es pirateada, todos nuestros datos serían robados" es una descripción de un impacto, no de un riesgo [11]. Los controles que faltan son las vulnerabilidades existentes, que pueden o no ser relevantes para el riesgo [11]. La probabilidad es la combinación de una amenaza y una vulnerabilidad [11]. Las declaraciones de riesgo deben incluir probabilidades e impactos calculados para proporcionarle los datos que necesita para realizar compensaciones [11]. Calcular la posibilidad de que algo suceda tiene dos elementos principales: la probabilidad de que una amenaza actúe y la probabilidad de que la amenaza aproveche una vulnerabilidad en los sistemas [11].

El riesgo fluye de los objetivos comerciales o de las partes de la organización que hacen dinero, interactúan con los clientes y / o hacen algo útil, los impactos se relacionan con los activos. Los activos pueden ser tangibles, como dinero, personas, instalaciones y sistemas de información. Los activos también pueden ser intangibles como la reputación, la propiedad intelectual, los contratos o la ventaja competitiva. Los activos son cualquier cosa que una organización considere valiosa [11].

Análisis de riesgos: es el proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización. Sabiendo lo que podría pasar, hay que tomar decisiones [10].

El análisis también es más que una simple lista de escenarios de desastre. Las declaraciones sobre "lo que podría salir mal" son los impactos, que no significan nada sin una probabilidad adjunta [11]. El análisis de riesgos provee información acerca de las amenazas reales para una organización [11].

Al observar el impacto en los activos, se pueden dividir en violaciones de confidencialidad, integridad y disponibilidad. Algunos activos tienen una magnitud diferente de impacto para diferentes tipos de infracciones. Por ejemplo, una violación de la confidencialidad contra una base de datos de tarjetas de pago probablemente se consideraría un impacto de mayor magnitud que una pérdida de disponibilidad para esa misma base de datos. Tener el sistema fuera de servicio es malo, pero la filtración de todos los datos confidenciales en Internet es peor. Así como el análisis de riesgos implica hacer un análisis de impacto, hacer un análisis de impacto presupone un inventario de activos completo y oportuno. Para el análisis de riesgos, el inventario de activos es uno de los primeros pasos. Su objetivo es tener una lista priorizada de sus activos más importantes [11].

Una de las grandes decisiones que se debe tomar es si el análisis de riegos será cualitativo o cuantitativo. El análisis de riesgo cualitativo no usa valores tangibles, sino que usa medidas relativas como alta, media y baja. El análisis cuantitativo utiliza valores numéricos, como dólares, y puede implicar un poco de trabajo Cualitativo [11].

Árboles de ataque: una estrategia de análisis de riesgos consiste en descomponer una amenaza de alto nivel en objetivos intermedios y luego en acciones de ataque individuales. Esta estructura consiste en un árbol con nodos secundarios teniendo relaciones *AND* u *OR*. El nodo raíz es el objetivo del atacante. El nodo raíz se descompone en los objetivos secundarios y los objetivos secundarios se descomponen aún más hasta los nodos hoja que representan las acciones individuales del atacante [12].

Árboles protección: después de formalizar los árboles de ataque surgió la noción de agregar defensas en dichos árboles. Estos árboles son como árboles de ataque, pero extendido con posibles defensas en las hojas. Además de agregar hojas defensivas [13].

Las diferencias entre los dos tipos de árboles están en lo que representan los nodos. Un nodo en un árbol de ataque representa una vulnerabilidad, estas vulnerabilidades se especifican, pero cómo protegerlas queda fuera del análisis formal. Un árbol de protección por su lado puede producir un análisis de dónde las protecciones deben colocarse para obtener la mayor protección con un menor gasto de recursos. El nodo raíz de un el árbol de protección se corresponde directamente con el nodo raíz en un árbol de ataque, pero el resto de la estructura del árbol puede diferir extensamente [12].

Una vez identificados los riesgos asociados a los distintos procesos, es necesario establecer una metodología para medirlos y priorizarlos. A lo largo de este proceso se examina también la eficacia del control interno, identificando la parte del riesgo total que no está sometida a medidas eficaces de mitigación. Se trata por tanto de delimitar, dentro

del riego inherente – la indeterminación intrínseca de la actividad, sin considerar la existencia de los controles existentes o que se puedan implantar para mitigarlo -, el riesgo residual, la variabilidad remanente que está asumiendo la empresa en una actividad y momento concretos, a pesar de los controles que en su caso se hayan establecido a tal efecto

Tratamiento de los riesgos: es el proceso destinado a modificar el riesgo [10]. Hay múltiples formas de tratar un riesgo entre las que se incluyen:

- Ignorar el riesgo, fingir que no se ha visto el riesgo y esperar que desaparezca
- Aceptar el riesgo y esperar que nunca ocurra o aceptando que pudiera ocurrir y previendo recursos para actuar cuando sea necesario
- Eliminar el riesgo o la actividad riesgosa y evitar las circunstancias que lo provocan
- Reducir el riesgo a través de los controles, reducir las posibilidades de que ocurra y acotar sus consecuencias,
- Compartir o transferir el riego, con otra organización, típicamente contratando un servicio o un seguro de cobertura, o, en última instancia.

Monitoreo: es poco probable que un control reduzca el riesgo a cero. Por lo tanto, una vez que los controles se implementan y se ejecutan, se debe monitorear su efectividad y adecuación. Estas son dos medidas diferentes. La efectividad mide qué tan bien funciona un control dentro de la organización. La adecuación es medir cuánto ese control realmente reduce el riesgo. A menudo, las personas cometen el error de solo medir la efectividad, pero no mirar cuál es el resultado del esfuerzo de reducción de riesgos. Por ejemplo, “En los últimos tres meses, hemos reducido nuestra tasa de infección de *malware* en un 20% (adecuación). Nuestro control antivirus ahora está activo en todos los servidores, basado en la auditoría interna Q2 (efectividad) " [11].

Durante todo el proceso de monitoreo se examina también la eficacia de los controles internos, identificando la parte del riesgo total que no está sometida a medidas eficaces de mitigación. Es necesario delimitar **el riego inherente**, que no es otro más que el riesgo presente para las actividades sin considerar la existencia de los controles existentes o que se puedan implantar para mitigarlo, y también **el riesgo residual**, que es aquella porción de riesgo remanente que está asumiendo la empresa en una actividad y momento concretos, a pesar de los controles que en su caso se hayan establecido a tal efecto [5].

Con estos conceptos se puede indicar que seguridad es la capacidad que poseen las redes o los sistemas de información para resistir, con un nivel de confianza dado, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad,

autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que proporcionan dichas redes y sistemas ofrecen [10].

ISO 27005 es un conocido estándar de gestión riesgos de seguridad de la información. Las tareas en ISO 27005 incluyen la identificación, evaluación y priorización de riesgos. La gestión de riesgos debe ser un proceso recurrente de análisis y acciones sin fin, que consiste en fases que, cuando se implementan adecuadamente, permiten la continua mejora en la toma de decisiones y mejora del rendimiento. Una organización crea, recolecta, y procesa una cantidad significativa de información en múltiples formatos durante las actividades de gestión de riesgos de seguridad de la información. Es importante que la organización identifique la información que debe protegerse, así como el nivel de protección que debería ser provisto. Una organización no puede compartir todo ya que puede incluir información confidencial que puede arruinar la reputación o funcionamiento normal si se divulga a un tercero malicioso, toda organización tiene la responsabilidad de proteger esta información y garantizar su confidencialidad, integridad y disponibilidad [14], Conocer los riesgos a los cuales está sujeta la información es necesario para poder gestionarlos de manera adecuada, la correcta gestión de riesgos permitirá empresa tener un ambiente de trabajo propicio, minimizando los riesgos a niveles aceptables. La reducción de estos niveles se realizará mediante el uso de medidas de seguridad, que proporcionan un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad [10].

Puesto que la información se clasifica en base a su nivel de sensibilidad y el impacto para organización si la información es revelada, alterada, destruida sin la autorización correspondiente, la clasificación de la información facilita la tarea de decidir los controles de seguridad básicos para salvaguardarla [14]. Los controles clave deben identificarse como el resultado de una evaluación de arriba hacia abajo de los riesgos del negocio, la tolerancia al riesgo y es necesario conocer cuáles son requeridos para administrar o mitigar el riesgo del negocio [11].

1.6. Revisión del Estado del Arte

En esta sección se tratará sobre diversos estudios centrados en la gestión de riesgos, el uso del EGSI y la protección de datos con RGPD, con el fin de identificar la información provista previamente por diversos investigadores que avalen la factibilidad de combinar estos elementos, se utilizará los lineamientos dados por [15] para realizar el análisis necesario.

1.6.1. Desarrollo

Los elementos planteados de acuerdo con [15] para realizar la búsqueda de literatura son: Tema, Limites espacios temporales, palabras claves y subtemas.

El Tema seleccionado acorde con el presente estudio es: Gestión de Riesgos con ISO 27002, Esquema Gubernamental de Seguridad de la Información (EGSI) y Reglamento General de Protección de Datos (RGPD).

Es importante anotar que se usan las siglas RGPD debido a que a nivel de literatura la mayoría de los trabajos usan estas siglas en lugar de RGDP.

El límite espacio temporal es: Ecuador 2013, año de la versión inicial de EGSI.

Las palabras claves son: EGSI, RGPD, ISO 27002, Seguridad de la Información. Gestión de Riesgos, protección de datos.

Los subtemas elegidos son: Gestión de Riesgos, Esquema Gubernamental de Seguridad de la Información, Protección de datos, Reglamento General de Protección de Datos, RGPD.

Al realizar una búsqueda booleana en los motores de búsqueda se encontró un total de 2 trabajos que cumplían las características indicadas, por este motivo, se procedió a depurar la búsqueda, y eliminar las referencias al RGPD y cambiarlo por protección de datos, con esta nueva búsqueda se encontraron 20 trabajos, sin embargo, de estos, 11 cumplían las características necesarias indicadas en las palabras claves.

Es con los 11 trabajos de investigación que mejor se acoplan a la temática del presente trabajo, que se realiza la presente revisión del estado del arte.

Presentación general de resultados

Durante la revisión de literatura se encontraron 11 documentos estrechamente relacionados con el tema de investigación propuesto por el presente trabajo. Estos textos se agrupan de acuerdo con sus características en:

- Grupo 1, Marcos de referencia y guías de implementación del EGSI, todos los documentos que proponen marcos de referencia o guías para una adecuada implementación del EGSI, cubriendo las etapas desde el diseño hasta la implementación de estos trabajos.
- Grupo 2, Análisis y propuestas de políticas para el uso del EGSI, aquellos documentos que elaboran políticas a seguir con el fin de iniciar una correcta implementación del EGSI, estas políticas pueden incluir o no controles de seguridad.
- Grupo 3, Seguridad de la información considerando la norma del EGSI, los trabajos que proponen un esquema de seguridad, evaluando riesgos, enmarcados en el

EGSI, considerando las etapas para una gestión adecuada de mencionados riesgos.

- Grupo 4, Estudio del EGSI, aquellas investigaciones, que realizan un análisis teórico del EGSI, revisando su normativa y base técnica.
- Grupo 5, Consideraciones sobre la protección de datos RGPD, este grupo es el más importante para el presente estudio, pues son los documentos que consideran la protección de datos enmarcada en el RGPD. Proponiendo un grupo de controles para el adecuado manejo de la información personal sensible

Descripción de factores

Una vez establecidos los grupos generales y sus características, de acuerdo con [15] es necesario un análisis más profundo de cada ítem. De esta manera se tiene:

La principal contribución de los textos categorizados en el grupo 1: [16] y [17], consiste en implementar procedimientos para el uso adecuado del EGSI en las instituciones públicas, de estos textos cabe recalcar que en [17] se realiza una priorización de los dominios de seguridad a validar y la guía es usada en una implantación real en la Agencia de Regulación y Control de la Electricidad. Como vació en estos trabajos tenemos la ausencia de una adecuada gestión de riesgos y la protección de los datos sensibles que se manejaran.

Los documentos en el grupo 2: [18], [22], [23], [26], contribuyen principalmente al establecer las políticas de seguridad necesarias que una organización debe utilizar para cumplir para estar alienadas con el EGSI, es importante anotar que de estos documentos en [18] y [26] se realiza una propuesta de controles de seguridad más detallada que pretende apoyar la implementación de EGSI. Si alineamos estos trabajos con la presente investigación, se puede apreciar, que carecen de un ciclo de gestión de riesgos, así como también la consideración de controles de seguridad que apoyen la protección de datos sensibles de los actores en los sistemas de información.

Los textos incluidos dentro grupo 3: [18], [19], [22], [23], [25], [26], son los que tienen una gran contribución al campo de estudio del presenta trabajo, tienen por principal característica el considerar EGSI como una parte esencial dentro de la implementación de propuestas de seguridad de la información, incluyendo análisis, evaluación y gestión de riegos dentro de un modelo de seguridad. De estos documentos cabe recalcar el aporte realizado en [25], que dentro de su modelo de seguridad lógica considera la protección de datos personales y sensibles haciendo uso del RGPD. Este grupo de trabajos se caracteriza por brindar un gran apoyo al presente trabajo, sin embargo, no presenta controles de seguridad específicos para apoyar la seguridad de los datos personales sensibles, únicamente provee lineamientos generales.

Los documentos incluidos en el grupo 4: [18] y [20], hacen un análisis del EGSI. El principal aporte de estas investigaciones es el presentar un marco técnico claro del EGSI, analizando incluso sus controles de seguridad propuestos, de estos trabajos se debe recalcar que en [20] el estudio llega incluso a validar el nivel de cumplimento de EGSI en el Ministerio de Educación. Este grupo de documentos son los que menos aportan en relación con la investigación propuesta, no existes manejo de riesgos, ni control sobre los datos personales sensibles.

Finalmente, los documentos del grupo 5: [21], [24] y [25], hacen el importante aporte de incluir de la protección de datos personales dentro de sus trabajos, considerando de manera prioritaria el entender lo vital que resulta para los sistemas de información proteger los datos sensibles de sus actores, enfocando dicha protección como parte de la seguridad de la información. De este grupo en importante recalcar la contribución de [21] al proponer una serie de controles de seguridad para considerar la protección de datos personales dentro del esquema de seguridad de la información y utilizando como referencia el RGPD. El principal vacío que presentan estos trabajos es no incluir un ciclo de gestión de riesgos alineado con la protección de datos personales sensibles. En la Tabla 1 se presenta el resumen del estado del arte.

Tabla 1 - Resumen estado del arte

TRABAJO	**AÑO**	**GESTIÓN DE RIESGOS**	**EGSI**	**PROTECCIÓN DE DATOS SENSIBLES**
José Pino [16]	2014		X	
Carolina Cáceres y Cristian Mena [17]	2015		X	
Alejandra Pinto [18]	2016	X	X	
Hugo Gualotuña y Geovanna Quilumbaqui [19]	2016	X	X	
Christian Muyón, Teresa Guarda y Geovanni Ninahualpa [20]	2018		X	
Angel Yánez [21]	2018		X	X
Marco Gallardo [22]	2018	X	X	
Catherine López [23]	2019	X	X	
Aura Zambrano, Jessica Morales, Joselin Párraga y Sebastiana Loor [24]	2019			X
Patricio Vaca [25]	2019	X	X	X
María Perugachi [26]	2020	X	X	

Conclusiones en relación con la investigación

Tomando como fundamento la literatura encontrada, es importante anotar que la norma ISO/EC 27000, es de vital importancia dentro de las consideraciones para trabajar con

controles de seguridad de EGSI, pues este último está fundamentado en la mencionada norma.

También se puede apreciar que en los trabajos analizados. un conjunto mínimo considera la protección de datos y el RGPD y los que lo consideran no validan su propuesta en un ciclo de gestión de riesgos.

Es importante recalcar, que, si bien es cierto EGSI tiene varios estudios, su nivel de madurez en las instituciones aun es pequeño, y es necesario promover su uso adecuado incluyendo aspectos de protección de datos sensibles.

1.6.2. Conclusiones

Partiendo de la información recopilada, se utilizarán ciertos aspectos de la propuesta de controles de seguridad basados en la protección de datos [21]. Se identifico que no existen trabajos que incluyan un ciclo de gestión de riesgos utilizando árboles de ataque y defensa, con lo cual el presente trabajo de investigación aportará en este sentido. Finalmente, otro aporte será el de validar como mejora la gestión de riesgos al incorporar controles de seguridad que consideren la protección de datos.

Para referencia de los documentos usados revisar el ANEXO I.

1.7. Motivación y contribución

El presente trabajo tiene como objetivo proponer un Ciclo de Gestión de Riesgo, que haga uso de los lineamientos provistos por el estándar ISO 27005, tomando en cuenta los controles propuestos por ISO 27002/ EGSI y considerando el RGPD europeo.

Para recorrer la fase de análisis de amenazas se plantea usar el modelado de amenazas automatizado, para identificar amenazas dentro del escenario propuesto.

Tanto el catálogo de amenazas como los actores de amenaza detectados servirán como entrada para la generación de los árboles de ataque y sus correspondientes de defensa, que se utilizarán para cuantificar los riesgos dentro del proceso de gestión.

Una vez cuantificado el riego se procederá a realizar el control y tratamiento de este mediante la implementación de nuevos controles de seguridad basados en EGSI y RGPD con el fin de iniciar un ciclo de mejora que permita validar si los controles propuestos reducen la incidencia de los riesgos detectados, para con esta validación proceder a monitorear y a analizar tanto el riesgo inherente como el riesgo residual.

El resultado final presentará un esquema de evaluación y mitigación de Riesgos que incorpora modelado de amenazas y mitigaciones automatizadas basadas en controles de seguridad según la ISO 27002/EGSI y RGPD.

Es importante indicar que el presente trabajo constituirá en un procedimiento con instrucciones paso a paso que permitan soportar las guías entregadas por el estándar ISO 27005.

2. METODOLOGÍA

La metodología del presente trabajo se basa en la metodología de investigación en ciencias del diseño para la investigación de sistemas de información presentada por Pers, Tuunanen, Rothenberger [27].

Esta metodología define las siguientes seis tareas:

a. Identificar el problema y motivación.
b. Definir los objetivos para una solución.
c. Diseño y desarrollo.
d. Demostración
e. Evaluación
f. Comunicación

De manera práctica estas tareas, y por lo tanto el presente trabajo, se pueden idear en tres fases.

Primera fase: consiste en definir el problema y descubrir qué se puede usar para definir objetivos y luego definir dichos objetivos, en este paso, se utilizará la búsqueda sistemática de ataques a los sistemas de información por medio de Internet, para con esto plantear un escenario que nos permitirá generar los catálogos de amenazas y perfiles de atacante que serán los objetivos por analizar.

Segunda fase: consiste en un proceso repetible de trabajo y demostración, en este paso se usarán de ítems la metodología cualitativa y cuantitativa. Se desea obtener las distintas matrices de riesgo, a partir de un catálogo de amenazas, en base a la norma ISO 27005 que constituyen la parte cualitativa del estudio, posteriormente se pretenden usar estas matrices como entradas de los distintos arboles de ataque y defensa que son parte integral de la metodología cuantitativa de análisis de riesgos.

Tercera fase: consiste en evaluar el trabajo, y presentar los resultados el mismo con sus conclusiones y propuestas de mejora. Una vez realizado el análisis cualitativo y cuantitativo de los vectores de ataque es necesario realizar una evaluación de estos y entregar resultados del modelo del Ciclo de riesgos, con estos resultados se pretende proponer controles adicionales fundamentados en el RGPD con el fin de evaluar nuevamente los riesgos por cada amenaza identificada y determinar el riesgo residual y el riesgo inherente, entregando los resultados finales del modelo propuesto.

2.1. Selección de Herramientas

La revisión sistemática de literatura [15] se usará para identificar reportes, casos de estudio y análisis de problemas que permitan identificar y proponer un escenario en el que sistemas de información (hardware-software y personas) son potencialmente comprometidos afectando la seguridad y privacidad de información.

Para trabajar la etapa de análisis de amenazas se plantea usar el modelado de amenazas mediante la herramienta *Microsoft Threat Modelling Tool* para identificar amenazas dentro del escenario propuesto. *Microsoft Thread Modeling Tool* utiliza el modelo de amenazas STRIDE, que es el modelo de amenazas más utilizado, usa las seis grandes categorías principales de amenazas: *Spoofing* (Suplantación), *Tampering* (Manipulación), *Repudiation* (Repudio), *Information Disclosure* (Divulgación de información), *Denial of Service* (denegación de servicio) y *Elevation of Privilege* (elevación de privilegios) [28].

STRIDE de Microsoft es una técnica de modelado de amenazas popular que se usa comúnmente para descubrir las debilidades de un sistema [28]. Microsoft ha documentado metodologías de modelado de amenazas desde 1999. Estos métodos han sido efectivos para encontrar fallas de seguridad en los diseños de productos, y se han incorporado al ciclo de vida de desarrollo de seguridad, un conjunto de procesos que se aplican a todos los productos de Microsoft con importantes riesgos de seguridad o privacidad [29].

La creación de árboles, tanto de ataque como de defensa, será mediante el uso de la herramienta *Attack-Defense Tree Tool* (ADTool).

La herramienta ADTool permite a los usuarios modelar y mostrar escenarios de ataque-defensa, mediante el uso de árboles de ataque-defensa, puede utilizar para automatizar y facilitar el uso de árboles de ataque-defensa. Además, ADTool permite realizar análisis cuantitativos en los nodos de los árboles creados. Esto significa que un usuario puede responder preguntas como: ¿Cuáles son los costos de un ataque, ¿cuál es el nivel mínimo de habilidad requerido? para el atacante, ¿cuánto tiempo lleva implementar todas las defensas necesarias o quién es el ganador del escenario de ataque-defensa considerado [30].

3. PROPUESTA DE CICLO DE GESTIÓN DE RIESGOS

La norma ISO 27005 contiene diferentes recomendaciones e indicaciones generales para la gestión de riesgo en los Sistemas de Gestión de Seguridad de la Información (SGSI). Es parte integral de los conceptos generales especificados en el estándar ISO 27001 y se encuentra diseñada como soporte para aplicar de forma satisfactoria un SGSI basado en el enfoque de gestión de riesgo [14].

El ciclo de gestión propuesto en presente trabajo se fundamenta en los lineamientos indicados por el estándar ISO 27005 y que se pueden apreciar en la Figura 1.

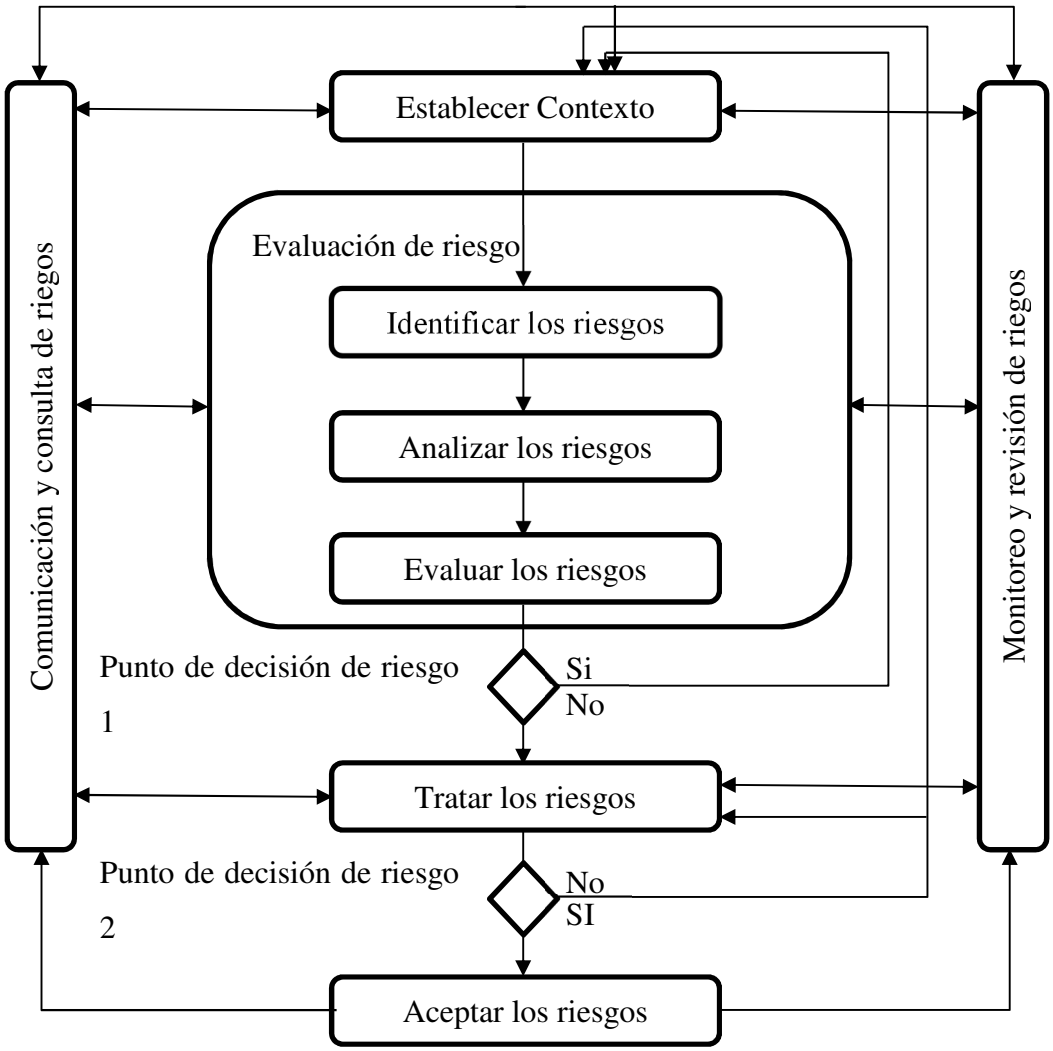


Figura 1 - Lineamientos ISO 27005 [14]

3.1. Fases de gestión de riesgos

Dentro del modelo de gestión propuesto La actividad “Tratar riesgos” del estándar ISO 27005 será dividida en control y tratamiento, con esta premisa al recorrer cada etapa de la norma ISO 27005, el ciclo de gestión de riesgos alineado al objetivo del presente trabajo se presenta en la Tabla 2.

Tabla 2 - Ciclo de gestión de riesgos propuestos

ISO 27005	ACTIVIDAD	ENTRADA	SALIDA
Establecer Contexto	Para definir el escenario del presente trabajo se ha procedido a realizar una búsqueda sistemática de eventos y brechas de seguridad a sistemas de información, que afecten datos personales sensibles	Reportes de brechas de seguridad encontrados en Internet. Modelo de sistema. Modelo de ataque.	Catálogo de amenazas en base a brechas usando Microsoft Threat Modelling Tool. Perfil de atacantes en base a los reportes de brechas.
Evaluación de riesgos	Para evaluar los riesgos, se utilizarán tanto el catálogo de amenazas, como los perfiles de atacantes, para crear arboles de ataque que permitan cuantificar el riesgo inherente.	Catálogo de amenazas. Perfil de atacantes.	Árboles de ataque. Riesgo inherente.
Control de riesgos	Para el control de los riesgos se plantea proponer controles de seguridad basado EGSI y RGPD.	Árboles de ataque. Riesgo inherente.	Controles de seguridad enfocados en la privacidad de datos.
Tratamiento de riesgos	Para tratar los riesgos encontrados, se propone usar arboles de defensa que utilizaran los controles de seguridad generados y con estos calcular el riesgo residual.	Controles de seguridad.	Arboles de defensa. Riesgo Residual.
Comunicación y validación	Para validar y realizar la comunicación dentro del ciclo se	Riesgo inherente. Riesgo residual	Comparación Riesgo inherente y Riesgo residual.

ISO 27005	ACTIVIDAD	ENTRADA	SALIDA
	compararán los riesgos: inherente y residual, para analizar la efectividad de los controles propuestos.		Análisis de efectividad.
Monitoreo	Como paso final de la primera etapa del ciclo de gestión de riesgos, se necesita revisar el análisis de efectividad y en base a este decidir si es necesario iniciar un nuevo ciclo dentro del proceso.	Análisis de efectividad	Iniciar un nuevo ciclo o aceptar el riesgo.

3.2. Esquema de gestión de riesgos

Tomando como base la Tabla 2, el ciclo de gestión propuesto tendría los lineamientos indicados en la Figura 2

.

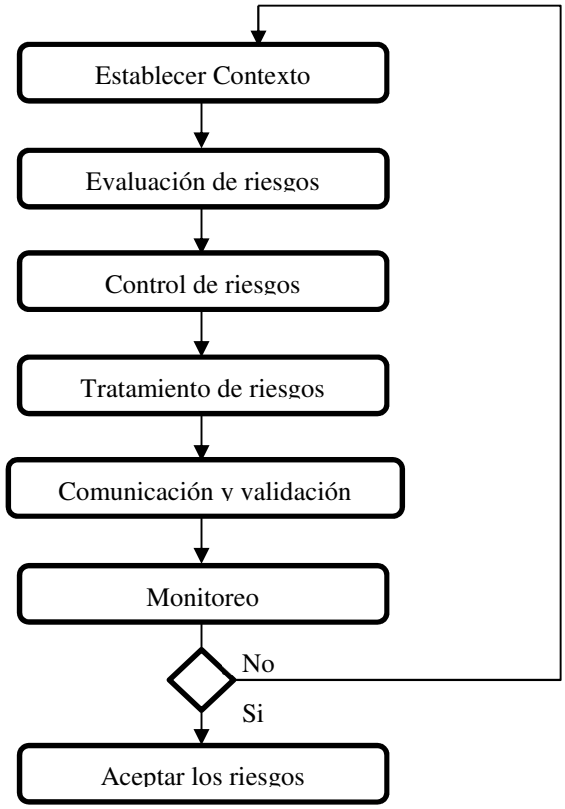


Figura 2 - Lineamientos ciclo de gestión propuesto

3.3. Evaluación y control de riesgos

Dentro de las etapas de evaluación de riesgo y control se consideran la generación de árboles de ataque y defensa, así como el uso de controles de seguridad basados en EGSI y RGPD.

3.3.1. Diseño y creación de árboles de ataque-defensa

Para el diseño y la creación de los árboles de ataque se utilizará la herramienta The Attack-Defense Tree Tool (ADTool).

El diseño y creación de los árboles se ha planteado en 4 etapas, según el método usado en [41]

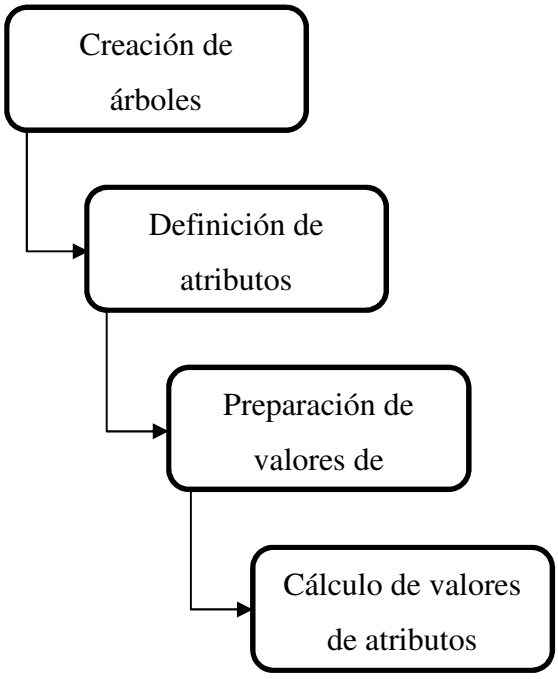


Figura 3 - Pasos para el diseño y creación de árboles de ataque [41]

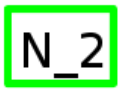
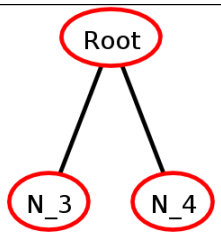
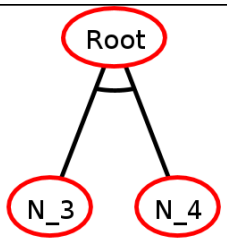
Los atributos comunes y sus valores correspondientes [12][41], para ser usados en los distintos árboles se indican en la Tabla 3.

Tabla 3 - Atributos comunes y valores generales

ATRIBUTO	DESCRIPCIÓN	VALOR
Costo [41]	La cantidad de dinero real necesario para financiar el ataque o defender contra él , refiriéndose, por ejemplo, a costos de equipo o software, gastos de educación, costos de desarrollo o tamaño de un soborno.	Barato (B) - 1 Moderado (M) - 2 Costoso (C) - 3
Impacto [12]	La severidad o consecuencia del propietario del sistema punto de vista. Puede referirse a pérdida de dinero, pero también otros recursos menos tangibles como pérdida de reputación.	1-3, Impacto menor en el sistema. 4-6, Impacto moderado en el sistema. 7-9, Impacto severo al sistema. 10, sistema completamente comprometido, inoperable o Destruido.
Probabilidad [12][41]	La supuesta factibilidad (*likelihood*) de que el ataque o la defensa tendrá éxito. Podría basarse en heurísticas de ataques similares o cognitivos estimaciones.	Improbable (I): por debajo del 5% (0.05). Bajo (B): Entre 5% y 25% (0.05 – 0.25). Medio (M): Entre el 25% y el 75% (0.25 – 0.75). Alto (A): más del 75%. Cierto (C): Cerca del 100% (1).
Habilidad	La habilidad técnica o social nivel necesario para el atacante o defensor para triunfar.	Muy Alto (MA) – 1.25 Alto (A) - 1 Medio (M) – 0.5 Bajo (B) – 0.25
Riesgo	Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización	$\frac{\text{Probabilidad x Habilidad}}{\text{Costo}}$ x Impacto

En la Tabla 4 se presenta la notación para el diseño y creación de árboles.

Tabla 4 - Notación ADTOOL

REPRESENTACIÓN GRAFICA	TIPO
	Nodo de ataque del árbol
	Contramedida
	Relación *OR*
	Relación *AND*

3.3.2. Controles de seguridad de información y protección de datos

Una parte fundamental dentro del ciclo de gestión propuesto son los controles de seguridad que cumplan con la normativa ISO 27000 y que consideren EGSI y el RGPD, considerando esto cada control de seguridad debe presentarse de acuerdo con "La Declaración de Aplicabilidad" de la norma ISO 27000.

En la Tabla 5 se presenta el ejemplo del formato de estado y aplicabilidad para un control de seguridad sugerido en base al EGSI y al RGPD y tomando como base controles propuestos en [21]. El listado completo de los controles a usar se encuentra en el Anexo II.

Tabla 5 - Ejemplo de control de seguridad basado en EGSI y RGPD

N°	CONTROL PROPUESTO	DESCRIPCIÓN	SECCIÓN ISO 27001:2013	SECCIÓN EGSI	SECCIÓN RGPD	PREGUNTAS
1	Establecer políticas para la gestión de datos personales sensibles	Establecer políticas revisadas y aprobadas por la Máxima autoridad de la Institución, que estipulen cuales son los datos personales sensibles que maneja la organización.	A 5.1.1 Políticas para la seguridad de la información	5.7.3 Aislar los servicios de procesamiento de información con datos sensibles y elementos que requieran protección especial, para reducir el riesgo de visualización de la información de personas no autorizadas.	El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. Se respeta la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de	¿La Institución posee prácticas, reglas, políticas o procedimientos definidos sobre el uso y la divulgación de datos personales que son de conocimiento de todos los actores del sistema de información? ¿La institución posee prácticas, reglas, políticas o procedimientos para el caso en que los usuarios del sistema de información pidieran justificación sobre todos los

N°	CONTROL PROPUESTO	DESCRIPCIÓN	SECCIÓN ISO 27001:2013	SECCIÓN EGSI	SECCIÓN RGPD	PREGUNTAS
					información, la libertad de empresa, expresión religiosa. 6. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.	datos personales que existe sobre ellos? ¿La Institución posee políticas o procedimientos definidos para determinar qué datos son sensibles respecto a los usuarios de los sistemas de información?

4. DEFINICIÓN DEL ESCENARIO TIPO DE AMENAZAS A LA SEGURIDAD Y PRIVACIDAD DE SISTEMAS DE INFORMACIÓN

Para definir el escenario del presente trabajo se ha procedido a realizar una búsqueda sistemática de eventos y brechas de seguridad a sistemas de información, que afecten datos personales sensibles, reportados desde el año 2016. Se ha elegido realizar este procedimiento con el fin de obtener un escenario real bastante completo en base a diversos reportes y eventos de brecha reportados, ya que al acceder a distintas fuentes se puede obtener un escenario mayor que al buscar el mismo en una sola empresa, pues cada empresa afectada solo notifica lo mínimo respecto a su vulneración, dejando el escenario incompleto, de esta manera al recolectar un número mayor de vulneraciones se tendrá un escenario más completo.

Siguiendo el método propuesto en [15], se utilizaron los siguientes valores:

- Tema: Brechas de seguridad que afectan datos personales sensibles.
- El límite espacio temporal: desde el 2016.
- Palabras claves: Brecha, seguridad, datos personales sensibles.
- Subtemas: brechas de seguridad, datos personales sensibles.

Al realizar una búsqueda de términos exactos y términos relacionados en títulos y capítulos en los motores de búsqueda se encontró un aproximado de 26.000 páginas que cumplían las características indicadas, por este motivo, se procedió a depurar la búsqueda reportes resumidos por año, un promedio de 1000 resultados, de estos se eliminaron reportes de blogs personales y revistas no involucradas con el área de la tecnología, de los resultados restantes se eligieron 5 noticias muy representativas ([31], [32], [33], [34] y [35]), que permiten la navegación a cada uno de los ítem reportados.

En base a los resultados elegidos de la búsqueda sistémica, se puede establecer el siguiente contexto para las brechas de seguridad que afectan datos personales sensibles.

En la Tabla 6, se presenta un resumen de las principales brechas detectadas en base a la búsqueda realizada y considerando el Modelo STRIDE que usa *Microsoft Threat Modelling Tool*.

Tabla 6 - Resumen de brechas de seguridad que afectaron datos sensibles

ORGANIZACIÓN	ACTIVOS COMPROMETIDOS	INFORMACIÓN SENSIBLE COMPROMETIDA	MÉTODO USADO O DEBILIDAD APROVECHADA	CATEGORÍA STRIDE	TIPO DE ATACANTE
Hard Rock Hotel & Casino [31]	Base de datos.	Datos de pagos de clientes, nombre, números de tarjetas de crédito, fechas de expiración.	Se utilizó *malware*, aprovechando la mala configuración de la red y falta de control de autenticación en el servidor con la base de datos.	Manipulación	Externo
Clash of Kings [31]	Sitio Web, base de datos.	Usuarios de acceso a aplicaciones, claves, Nombres.	El sitio web era obsoleto no usaba https, permitiendo a un usuario malicioso realizar operaciones no permitidas.	Elevación de Privilegios	Externo
Wendy's [31]	Puntos de venta, base de datos.	Datos de pagos de clientes, nombre, números de tarjetas de crédito, fechas de expiración.	Se utilizó *malware*, aprovechando la mala configuración de la red y falta de control de autenticación en el servidor con la base de datos.	Manipulación	Externo
Servicio Nacional de Salud del Reino Unido [32]	Base de datos. Servidores web.	Citas médicas, datos de pacientes, nombres, género, información de salud, direcciones físicas, correos electrónicos.	Se utilizó *ramsonware* aprovechando la mala configuración de la red.	Manipulación	Externo
Facebook [33]	Base de datos. Aplicación Web.	Tokens de acceso, datos personales, nombres, genero, fechas de nacimiento, ocupación, fotografías, contactos.	Vulnerabilidad en el código fuente, que permitía acceder a tokens de acceso sin necesidad de conectarse.	Manipulación	Externo
Marriot [33]	Base datos	Información personal y bancaria como: nombre,	Acceso no autorizado a la base de datos, debido a	Elevación de privilegios	Interno

ORGANIZACIÓN	ACTIVOS COMPROMETIDOS	INFORMACIÓN SENSIBLE COMPROMETIDA	MÉTODO USADO O DEBILIDAD APROVECHADA	CATEGORÍA STRIDE	TIPO DE ATACANTE
		números de tarjetas de crédito, fechas de expiración.	falta de configuración de seguridad en el servidor y en la base de datos.		
British Airways [33]	Base datos. Servidor. Sitio web. Aplicación móvil.	Información personal y bancaria como: nombre, números de tarjetas de crédito, fechas de expiración.	Vulnerabilidad en el servidor que albergaba código *javascript*, manipulando los datos del formulario de usuarios, permitiendo un ataque de secuencia de comandos.	Manipulación	Externo
Under Armour y MyFitnessPal [33]	Servidor web. Aplicación web	Nombres de usuario, direcciones de correo electrónico y contraseñas.	La aplicación permitía a los atacantes elevar sus privilegios y acceder a más información de la permitida por su rol.	Elevación de privilegios	Externo
Quora [34]	Servidor de aplicación.	Nombres, direcciones de correo, dirección IP, ID de usuarios, contraseñas cifradas, datos de configuración de las cuentas.	Accesos no autorizados a los sistemas por parte de terceros, mediante la personificación de la aplicación y falta de configuración de seguridad en el servidor.	Elevación de privilegios	Externo
Gobierno de Brasil [34]	Servidor web Apache.	Número de identificación financiera.	Mala configuración del servidor web permitió a los atacantes acceder a la información almacenada.	Elevación de privilegios	Externo
Exactis [34]	Base de datos pública en la nube.	Números de teléfono, dirección postal, dirección de correo electrónico.	La base de datos estaba en la nube en un servidor de acceso público.	Elevación de privilegios	Externo
Banco Caja Rural [35]	Base de datos.	DNI, clave de acceso a la entidad.	Acceso no autorizado a la base de datos, debido a falta de configuración de	Elevación de privilegios	Externo

ORGANIZACIÓN	ACTIVOS COMPROMETIDOS	INFORMACIÓN SENSIBLE COMPROMETIDA	MÉTODO USADO O DEBILIDAD APROVECHADA	CATEGORÍA STRIDE	TIPO DE ATACANTE
			seguridad en el servidor y en la base de datos.		
Sistema Médico de EEUU [35]	Servidores de base de datos.	Pruebas médicas.	Acceso no autorizado a los servidores de base de datos que están en la nube y sin seguridades básicas como usuario y clave.	Elevación de privilegios	Externo
Gobierno del Ecuador [35]	Servidor de base de datos en la nube.	Datos sensibles sobre relaciones personales, la situación financiera, salarios o incluso puestos de trabajo.	Acceso no autorizado a la base de datos en la nube, dentro de un servidor de acceso público.	Elevación de privilegios	Externo
Hostinger [35]	Base de datos. Servidor de aplicaciones.	Nombres de usuario, correo electrónico, contraseñas (aunque estaban hasheadas), direcciones IP, direcciones físicas y el número de teléfono.	Elevación de privilegios mediante un token de acceso, que se usó para obtener mayores privilegios de acceso y acceder a otras zonas del sistema sin contar con usuario y contraseña. Finalmente se accedió a la API del servidor, que contiene datos de los clientes de Hostinger.	Elevación de privilegios	Externo
Biostar 2 [35]	Servidor de base de datos en la nube.	Huellas dactilares de más de un millón de personas, así como información de reconocimiento facial, nombres de usuario y contraseñas e información de empleados.	Acceso no autorizado a la base de datos en la nueve mediante el uso de elasticsearch.	Elevación de privilegios	Externo

ORGANIZACIÓN	ACTIVOS COMPROMETIDOS	INFORMACIÓN SENSIBLE COMPROMETIDA	MÉTODO USADO O DEBILIDAD APROVECHADA	CATEGORÍA STRIDE	TIPO DE ATACANTE
Capital One [35]	Base de datos.	Números de la seguridad social números de cuenta, nombres, direcciones, datos de créditos o historia financiera.	Un usuario interno explotó un Firewall mal configurado para ingresar al servidor que contenía la base de datos.	Elevación de privilegios	Interno
Gobierno de Bulgaria [35]	Base de datos.	Nombres, información sobre ingresos, declaraciones fiscales, préstamos o seguros médicos.	Un ex consultor de la entidad aprovecho las malas configuraciones de los servidores para acceder a la base de datos.	Elevación de privilegios	Interno
Toyota [35]	Servidor de aplicación.	Números de teléfono, dirección postal, dirección de correo electrónico.	Accesos no autorizados a los sistemas por parte de terceros, mediante la personificación de la aplicación.	Elevación de privilegios	Externo
Gearbest [35]	Servidor web.	Correos electrónicos, contraseñas, perfiles de usuario, órdenes de compra, datos de métodos de pago.	La mala configuración del servidor que no contaba ni con contraseña, permitió el acceso a los datos almacenados.	Elevación de privilegios	Externo

Es importante indicar que tomando en consideración la Tabla 6, el principal objetivo de todos los ataques es “El robo de información sensible”, misma que en la actualidad es de gran valor, considerando este hecho, se procede a generar en la Tabla 7, un catálogo inicial de amenazas que provocan las brechas de seguridad que afectan datos personales sensibles.

Tabla 7 - Catálogo inicial de amenazas de brechas de seguridad que afectaron datos sensibles

ID	ACTIVOS COMPROMETIDOS	MÉTODO USADO O DEBILIDAD APROVECHADA	CATEGORÍA STRIDE	TIPO DE ATACANTE
A1	Base de datos.	Se utilizó m*alware* o *ramsonware*, aprovechando la mala configuración de la red y falta de control de autenticación en el servidor con la base de datos.	Manipulación	Externo
A2	Sitio Web, base de datos.	El sitio web era obsoleto no usaba https, permitiendo a un usuario malicioso realizar operaciones no permitidas.	Manipulación	Externo
A3	Base de datos. Aplicación Web.	Vulnerabilidad en el código fuente, que permitía acceder a tokens de acceso sin necesidad de conectarse.	Manipulación, repudio	Externo
A4	Base de datos. Aplicación Web.	Vulnerabilidad en el código fuente, que permitía realizar inyección SQL permitiendo al usuario elevar sus privilegios y manipular la información no permitida	Elevación de privilegios, Manipulación	Externo
A5	Base datos	Acceso no autorizado a la base de datos, debido a falta de configuración de seguridad en el servidor y en la base de datos.	Elevación de privilegios, Repudio, Suplantación	Externo
A6	Base datos. Servidor. Sitio web. Aplicación móvil.	Vulnerabilidad en el servidor que albergaba código *javascript*, manipulando los datos del formulario de usuarios, permitiendo un ataque de secuencia de comandos.	Manipulación	Externo
A7	Servidor web. Aplicación web	La aplicación permitía a los atacantes elevar sus privilegios y acceder a más información de la permitida por su rol.	Elevación de privilegios, Manipulación	Externo

ID	ACTIVOS COMPROMETIDOS	MÉTODO USADO O DEBILIDAD APROVECHADA	CATEGORÍA STRIDE	TIPO DE ATACANTE
A8	Servidor de aplicación.	Accesos no autorizados a los sistemas por parte de terceros, mediante la personificación de la aplicación y falta de configuración de seguridad en el servidor.	Elevación de privilegios	Externo
A9	Base de datos pública en la nube.	La base de datos estaba en la nube en un servidor de acceso público.	Divulgación de información	Externo
A10	Base de datos.	Un usuario interno explotó un Firewall mal configurado para ingresar al servidor que contenía la base de datos.	Elevación de privilegios	Interno

4.1. Modelo de sistema

En base a la Tabla 6, se propone una infraestructura experimental que permite analizar las potenciales amenazas que afectaron a las organizaciones que reportaron brechas de seguridad y que por motivos confidencialidad no fueron revelados de manera clara y total en los reportes analizados, se puede apreciar que se omiten detalles muchas veces importantes. Sin embargo, al juntar todos los reportes se obtiene una visión más completa y detallada de los sistemas afectados.

Partiendo de la información recolectada, se define la infraestructura común para las diferentes instituciones afectadas por brechas de seguridad.

- Servidores de bases de datos, con configuración de seguridad baja o nula, muchas veces sin uso de contraseñas.
- Motores de base de datos, con baja auditoría, y seguridades bajas, manejando los datos personales sensibles sin encriptar.
- Servidor web, que no usan https, con configuración de seguridad baja o nula, muchas veces sin uso de contraseñas.
- Sitios o aplicaciones web, que utilizan para personificarse usuario con altos privilegios del servidor en el que se ejecutan, sin adecuado manejo de los datos sensibles que utilizan, sin la programación adecuada que dificulte la inyección de código SQL o ataques por secuencia de comandos.
- Servidores fuera de la compañía, en manos de terceros para almacenar copias de la base de datos o las aplicaciones, que permiten accesos públicos.
- Browser o dispositivos móviles, son los medios de acceso desde el exterior a los servicios prestados.

- Los sistemas analizados tienen usuarios internos y externos.

Utilizando *Microsoft Threat Modeling Tool* 2016, en la Figura 4, se modela la infraestructura experimental, este modelado permite enriquecer el escenario propuesto de manera que permita analizar las posibles amenazas que afectaron a las organizaciones.

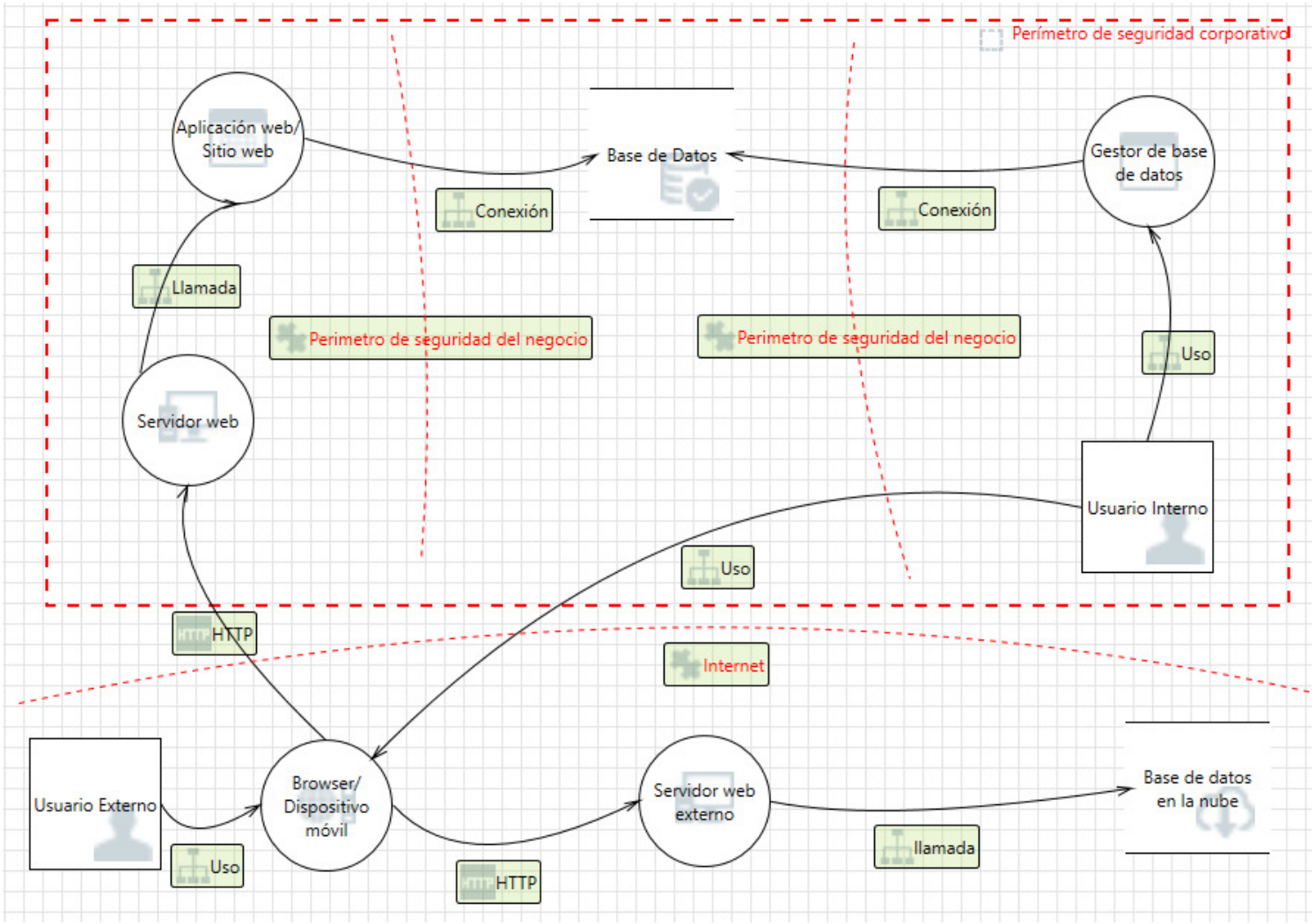


Figura 4 - Infraestructura de organizaciones afectadas

4.2. Modelo de ataque

Considerando la Tabla 6 y la Figura 4, se puede describir el siguiente modelo de ataque:
Un usuario externo puede aprovechar una mala configuración en los servidores, para atacar los mismos con *malware* o *ramsonware*, que le permite tomar control del servidor y acceder a los archivos de base de datos.
Un usuario externo puede aprovechar la falta de uso de https para atacar los servidores web y realizar manipulación hasta obtener los archivos de base de datos.
Un usuario externo aprovechando código fuente mal programado en la aplicación web, puede realizar un ataque de secuencia de comando o inyección de SQL, que le permite alterar el flujo de ejecución del programa accediendo a información en la base de datos que no le corresponde, así mismo por mala configuración de la aplicación el mismo usuario puede usar la personificación que usa esta, para elevar sus privilegios y acceder a los servidores y por ende a la base de datos.
Un usuario externo, puede realizar búsquedas en la red y encontrar servidores públicos de libre acceso que almacenan copias de la base de datos y las colocan en la nube, de esta manera se puede acceder a todos los archivos de la base de datos.
Usuarios internos pueden acceder a servidores que no les corresponde elevando sus privilegios al aprovechas firewall mal configurados o usar claves que deberían estar caducadas.

5. EVALUACIÓN DEL CICLO DE GESTIÓN DE RIESGOS

Tomando en cuenta el escenario tipo de estudio, se realizará un ciclo de gestión de riesgos, recorriendo cada una de las etapas propuestas.

5.1. Establecer contexto

En el ciclo de gestión de riesgos propuesto la primera fase consiste en “Establecer el contexto”, para una mejor comprensión y orden en el capítulo anterior se definió el escenario tipo en base a la búsqueda de ataques reportados, con este escenario tipo se puede establecer de manera general 2 puntos importantes:

1.) Modelo del sistema, que define la infraestructura común a utilizar, consistente en:
    a. Servidores de bases de datos, con configuración de seguridad baja o nula, muchas veces sin uso de contraseñas.
    b. Motores de base de datos, con baja auditoría, y seguridades bajas, manejando los datos personales sensibles sin encriptar.
    c. Servidor web, que no usan https, con configuración de seguridad baja o nula, muchas veces sin uso de contraseñas.
    d. Sitios o aplicaciones web, que utilizan para personificarse usuario con altos privilegios del servidor en el que se ejecutan, sin adecuado manejo de los datos sensibles que utilizan, sin la programación adecuada que dificulte la inyección de código SQL o ataques por secuencia de comandos.
    e. Servidores fuera de la compañía, en manos de terceros para almacenar copias de la base de datos o las aplicaciones, que permiten accesos públicos.
    f. Browser o dispositivos móviles, son los medios de acceso desde el exterior a los servicios prestados.
    g. Los sistemas analizados tienen usuarios internos y externos.
2.) Modelo de ataque, que indica la manera en que el sistema de información puede verse afectado y que a manera de resumen consiste en:
    a. Un usuario externo puede aprovechas errores de programación o mala configuración de los equipos para cambiar el flujo del programa mediante secuencias de comando, inyección de SQL o elevación de privilegios, para de esta forma acceder a los archivos de base de datos, o también mediante el uso de códigos maliciosos.

b. Un usuario externo, puede realizar búsquedas en la red y encontrar servidores públicos de libre acceso que almacenan copias de la base de datos y las colocan en la nube, de esta manera se puede acceder a todos los archivos de la base de datos.
c. Usuarios internos maliciosos puede aprovechar malas configuraciones internas o claves caducadas para elevar sus privilegios y acceder a los archivos de base de datos.

Con el escenario tipo definido es necesario estratificar tanto los perfiles del atacante como el catálogo de amenazas.

5.1.1. Perfil de atacantes

Usando el método propuesto en [36], [37] y [38] y en base a la información recolectada de los casos de brechas de seguridad reportados, se hace una primera división de los atacantes 2 grupos.

- Atacantes Internos, aquellos que pertenecen a la organización afectada, que por motivos personales o financieros realizan la extracción de datos sensibles usando sus credenciales con fines perniciosos y aprovechando la mala configuración y seguridad de los equipos. En la Figura 5 se puede apreciar los casos de mal uso de un atacante interno.

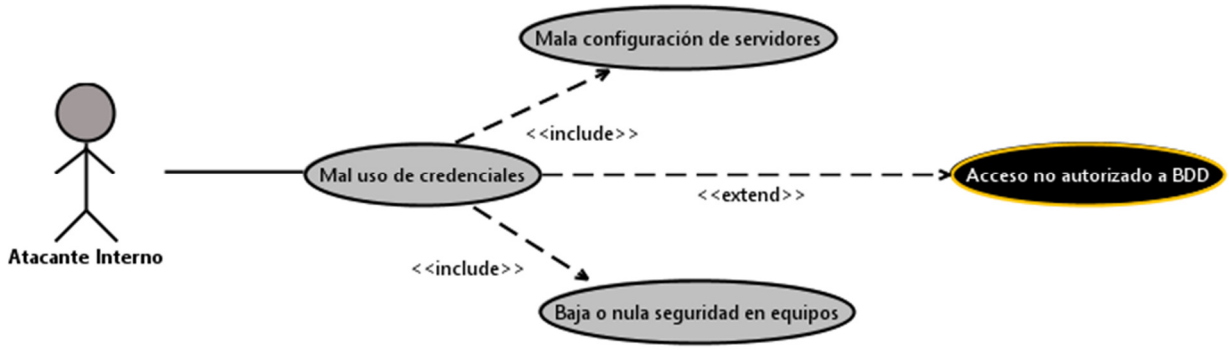


Figura 5 - Diagrama de casos de mal uso de atacantes internos

- Atacantes externos, aquellas personas que desde fuera de la organización afectada realizan sus ataques por motivaciones ideológicas o económicas, aprovechando la mala configuración de servidores internos o la mala programación de las aplicaciones empresariales vulnera el sistema o en su defecto buscan servidores públicos que les permitan acceder a la información compartida en la nube. En la Figura 6 se presenta el diagrama de casos de mal uso de los atacantes externos.

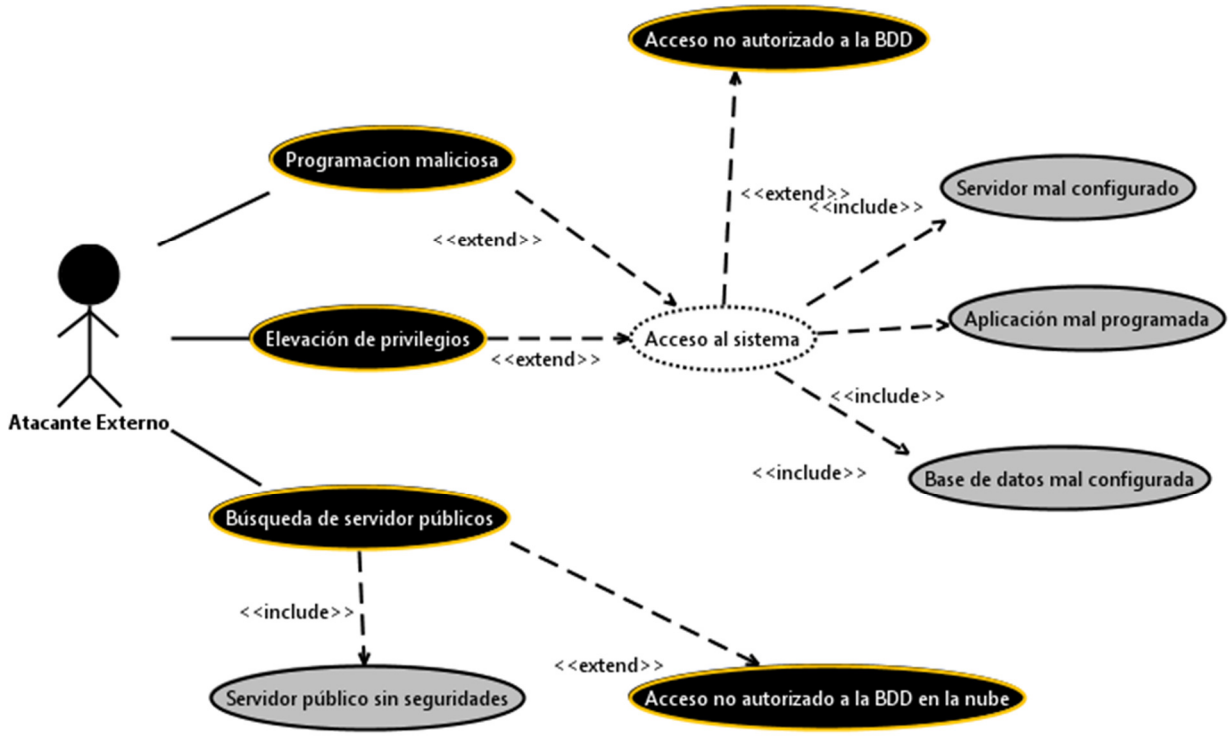


Figura 6 - Diagrama de casos de mal uso de atacantes externos

Es necesario parametrizar estos grupos de atacantes para lo cual se utilizará la Tabla 8, en base a [39], [40] y [41].

Tabla 8 - Parámetros generales de perfiles de atacantes

PARÁMETRO	DESCRIPCIÓN	VALORES
Habilidad	Nivel de habilidad de los atacantes para efectuar su labor.	Muy Alto (MA) Alto (A) Medio (M) Bajo (B)
Presupuesto	Cantidad de recursos financieros disponibles para el atacante.	Barato (B) - 1 Moderado (M) - 2 Costoso (C) - 3
Tiempo	Cantidad de tiempo, que el atacante puede invertir en su ataque.	Segundos (S), Minutos (M), Horas (H), Días (D).

- Atacantes Internos, al estar al interior de la organización sus habilidades son de nivel medio y alto, el tiempo disponible es de días y al tener casos reportados exitosos se evidencia que el presupuesto monetario fue el suficiente y se considera como moderado.

- Atacantes externos, al encontrarse fuera de la organización sus habilidades son de nivel cuando menos medios y pueden llegar a altos, el tiempo disponible es de días en la mayoría de los reportes de brechas y al tener casos reportados exitosos se evidencia que el presupuesto monetario fue el suficiente y se considera como moderado.

En la Tabla 9 se presenta el resumen del perfil de atacantes.

Tabla 9 - Perfiles de atacantes del contexto de seguridad

ATACANTES	HABILIDAD	PRESUPUESTO USD	TIEMPO
Internos	M – A	M	D
Externos	M – A	M	D

Al considerar los perímetros de seguridad existentes indicados en la Figura 4, se observa que los atacantes externos están en el perímetro de internet, aprovechando malas configuraciones de los equipos y errores de programación, para de esta manera obtener lo que buscan, Por otro lado, los atacantes internos están dentro del perímetro corporativo, pero fuera del de negocio, para lo cual mal usan credenciales y explotan malas configuraciones de seguridad.

5.1.2. Refinamiento catálogo de amenazas

De acuerdo con el modelo de ataque, se puede ver que tanto atacantes externos, como internos aprovechan malas configuraciones de los equipos, ausencias de seguridades, no uso de https para poder realizar sus actividades.

Los usuarios externos maliciosos también pueden usar sus conocimientos e identificar errores de programación para vulnerar los programas y ejecutar sus ataques.

Para usuarios externos también existe la posibilidad de realizar búsquedas de servidores públicos no protegidos para poder acceder a la información que buscan.

Para el modelado de amenazas se realizó un proceso automatizado, con el uso *Microsoft Thread Modeling Tool* 2016, utilizando como punto de partida la infraestructura propuesta y el esquema de ataque, en base a la revisión de brechas de seguridad.

Como se indicó en secciones anteriores *Microsoft Thread Modeling Tool* utiliza el modelo de amenazas STRIDE [28][29][42], al ejecutar la herramienta se obtiene el catálogo de Amenazas, que se puede revisar con detalle en el Anexo III.

Es posible enriquece el catálogo de amenazas automatizadas obtenido con los valores de la Tabla 5, misma que contiene las amenazas conseguidas en base a la revisión de literatura, es importante anotar que al estar en escenario de amenazas que afectan a la

privacidad de la información, los registros correspondientes a denegación de servicio o que afecten al navegador o dispositivo externo sin afectar los equipos internos, no serán consideradas, pues estas no llegan al objetivo de los ataques que es apoderarse de los archivos existentes en la base de datos.

Al combinar la Tabla 7 y el catálogo de amenazas generado con *Microsoft Thread Modeling Tool*, más las consideraciones indicadas, se obtiene en la Tabla 10, el catálogo de amenazas a la privacidad de la información.

Tabla 10 - Catálogo de amenazas a la privacidad de la información

ID AMENAZA	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	DESCRIPCIÓN	ID INICIAL	DESCRIPCIÓN	TIPO	ATACANTE
B13	El servidor web puede estar sujeto a la elevación de privilegios mediante la ejecución remota de código	Servidor Web	Elevación de privilegios	El navegador / Dispositivo móvil puede hacerse pasar por el contexto de Usuario Externo para obtener privilegios adicionales.	A7	La aplicación permitía a los atacantes elevar sus privilegios y acceder a más información de la permitida por su rol.	Elevación de privilegios, Manipulación	Externo
B14	Elevación cambiando el flujo de ejecución en Servidor web	Servidor Web	Elevación de privilegios	Aplicación web / Sitio web puede hacerse pasar por el contexto de Servidor web para obtener privilegios adicionales.	A8	Accesos no autorizados a los sistemas por parte de terceros, mediante la personificación de la aplicación y falta de configuración de seguridad en el servidor.	Elevación de privilegios	Externo
B15	Elevación mediante suplantación	Base de Datos	Elevación de privilegios	Base de Datos puede ser falsificada por un atacante y esto puede llevar a que los datos se escriban en el objetivo del atacante en lugar de Base de	A5	Acceso no autorizado a la base de datos, debido a falta de configuración de seguridad en el servidor y	Elevación de privilegios, Repudio, Suplantación	Externo

				Datos. Considere utilizar un mecanismo de autenticación estándar para identificar el almacén de datos de destino.		en la base de datos.		
B16	Elevación mediante suplantación	Aplicación Web	Elevación de privilegios	La inyección SQL es un ataque en el que se inserta código malicioso en cadenas que luego se pasan a una instancia de SQL Server para su análisis y ejecución. Cualquier procedimiento que construya declaraciones SQL debe revisarse para detectar vulnerabilidades de inyección porque SQL Server ejecutará todas las consultas sintácticamente válidas que reciba. Incluso los datos parametrizados pueden ser	A4	Vulnerabilidad en el código fuente, que permitía realizar inyección SQL permitiendo al usuario elevar sus privilegios y manipular la información no permitida	Elevación de privilegios, Manipulación	Externo

				manipulados por un atacante hábil y decidido.				
B18	Elevación mediante suplantación	Base de Datos	Elevación de privilegios	Usuario Interno puede ser engañado por un atacante y esto puede dar lugar a un acceso no autorizado al Gestor de base de datos. Considere utilizar un mecanismo de autenticación estándar para identificar la entidad externa.	A5	Acceso no autorizado a la base de datos, debido a falta de configuración de seguridad en el servidor y en la base de datos.	Elevación de privilegios, Repudio, Suplantación	Externo
B19	Elevación mediante suplantación	Base de Datos	Elevación de privilegios	Gestor de base de datos puede hacerse pasar por el contexto de Usuario Interno para obtener privilegios adicionales.	A10	Un usuario interno explotó un Firewall mal configurado para ingresar al servidor que contenía la base de datos.	Elevación de privilegios	Interno

B20	El navegador / dispositivo móvil puede estar sujeto a la elevación de privilegios mediante la ejecución remota de código	Base de Datos	Elevación de privilegios	Base de Datos puede ser falsificada por un atacante y esto puede llevar a que los datos se escriban en el objetivo del atacante en lugar de Base de Datos. Considere utilizar un mecanismo de autenticación estándar para identificar el almacén de datos de destino.	A5	Acceso no autorizado a la base de datos, debido a falta de configuración de seguridad en el servidor y en la base de datos.	Elevación de privilegios, Repudio, Suplantación	Externo
B21	Elevación al cambiar el flujo de ejecución en el navegador / dispositivo móvil	Aplicación Web	Elevación de privilegios	La inyección SQL es un ataque en el que se inserta código malicioso en cadenas que luego se pasan a una instancia de SQL Server para su análisis y ejecución. Cualquier procedimiento que construya declaraciones SQL debe revisarse para detectar vulnerabilidades de inyección porque SQL Server ejecutará todas las	A4	Vulnerabilidad en el código fuente, que permitía realizar inyección SQL permitiendo al usuario elevar sus privilegios y manipular la información no permitida	Elevación de privilegios, Manipulación	Externo

				consultas sintácticamente válidas que reciba. Incluso los datos parametrizados pueden ser manipulados por un atacante hábil y decidido.				
B25	Detección de flujo de datos	Servidor Web Externo	Divulgación de información	El servidor web 'Servidor web externo' podría estar sujeto a un ataque de scripting entre sitios porque no desinfecta la entrada que no es de confianza.	A9	La base de datos estaba en la nube en un servidor de acceso público.	Divulgación de información	Externo
B26	Tránsito de credenciales débil	Servidor Web Externo	Divulgación de información	Servidor web externo puede hacerse pasar por el contexto de Navegador / Dispositivo móvil para obtener privilegios adicionales.	A9	La base de datos estaba en la nube en un servidor de acceso público.	Divulgación de información	Externo
B27	Detección de flujo de datos	Aplicación Web	Divulgación de información	Aplicación web / Sitio web puede ser falsificado por un atacante y esto puede dar lugar a un acceso no autorizado	A8	Accesos no autorizados a los sistemas por parte de terceros, mediante la	Elevación de privilegios	Externo

				a Base de Datos. Considere utilizar un mecanismo de autenticación estándar para identificar el proceso de origen.		personificación de la aplicación y falta de configuración de seguridad en el servidor.		
B30	Data Store niega que la base de datos pueda escribir datos	Base de Datos	Repudio	Un atacante puede rastrear los datos que fluyen a través de Conexión. Dependiendo del tipo de datos que pueda leer un atacante, puede usarse para atacar otras partes del sistema o simplemente ser una divulgación de información que conduce a violaciones de cumplimiento. Considere cifrar el flujo de datos.	A5	Acceso no autorizado a la base de datos, debido a falta de configuración de seguridad en el servidor y en la base de datos.	Elevación de privilegios, Repudio, Suplantación	Externo

B31	Posible rechazo de datos por parte del navegador / dispositivo móvil	Aplicación Web	Repudio	Las credenciales en un mensaje a menudo están sujetas a ser detectadas por un atacante. ¿Las credenciales son reutilizables / reproducibles? ¿Se incluyen las credenciales en un mensaje? Por ejemplo, enviando un archivo zip con la contraseña en el correo electrónico. Utilice criptografía sólida para la transmisión de credenciales. Utilice las bibliotecas del sistema operativo si es posible y considere la agilidad del algoritmo criptográfico, en lugar de codificar una opción.	A3	Vulnerabilidad en el código fuente, que permitía acceder a tokens de acceso sin necesidad de conectarse.	Manipulación, repudio	Externo
B33	Suplantación del proceso web del servidor	Servidor Web	Suplantación	Un agente externo evita el acceso a un almacén de datos en el otro lado del límite de confianza.				

B34	Suplantación de la entidad externa Usuario Externo	Base de Datos	Suplantación	Gestor de base de datos puede ser falsificado por un atacante y esto puede dar lugar a un acceso no autorizado a Base de Datos. Considere utilizar un mecanismo de autenticación estándar para identificar el proceso de origen.	A5	Acceso no autorizado a la base de datos, debido a falta de configuración de seguridad en el servidor y en la base de datos.	Elevación de privilegios, Repudio, Suplantación	Externo
B35	Suplantación de la base de datos del almacén de datos de destino	Base de Datos	Suplantación	Los datos que fluyen a través de Conexión pueden ser manipulados por un atacante. Esto puede conducir a la corrupción de la Base de Datos. Asegure la integridad del flujo de datos al almacén de datos.				
B39	Suplantación del proceso Aplicación web / Sitio web	Aplicación Web	Suplantación	Un agente externo interrumpe el flujo de datos a través de un límite de confianza en cualquier dirección.				

B43	Posible falta de validación de entrada para el servidor web	Servidor Web	Manipulación	Los datos que fluyen a través de Uso pueden ser manipulados por un atacante. Esto puede dar lugar a un ataque de denegación de servicio contra el navegador / dispositivo móvil o un ataque de elevación de privilegios contra el navegador / dispositivo móvil o una divulgación de información por parte del navegador / dispositivo móvil. No verificar que la entrada sea la esperada es la causa principal de una gran cantidad de problemas explotables. Conside re todas las rutas y la forma en que manejan los datos. Verifique que se verifique que todas las entradas sean correctas utilizando un enfoque de validación de	A2	El sitio web era obsoleto no usaba https, permitiendo a un usuario malicioso realizar operaciones no permitidas.	Manipulación	Externo

				entradas de lista aprobada.				
B44	Secuencias de comandos entre sitios	Aplicación Web	Manipulación	Browser / Dispositivo móvil afirma que no recibió datos de una fuente fuera del límite de confianza. Considere utilizar el registro o la auditoría para registrar la fuente, la hora y el resumen de los datos recibidos.	A6	Vulnerabilidad en el servidor que albergaba código *javascript*, manipulando los datos del formulario de usuarios, permitiendo un ataque de secuencia de comandos.	Manipulación	Externo

B45	Potencial vulnerabilidad de inyección de SQL para la base de datos	Aplicación Web	Manipulación	Los datos que fluyen a través de Uso pueden ser olfateados por un atacante. Dependiendo del tipo de datos que pueda leer un atacante, puede usarse para atacar otras partes del sistema o simplemente ser una divulgación de información que conduce a violaciones de cumplimiento. Considere cifrar el flujo de datos.	A4	Vulnerabilidad en el código fuente, que permitía realizar inyección SQL permitiendo al usuario elevar sus privilegios y manipular la información no permitida	Elevación de privilegios, Manipulación	Externo
B46	Potencial vulnerabilidad de inyección de SQL para la base de datos	Navegador / Dispositivo Móvil	Manipulación	El navegador / Dispositivo móvil se bloquea, se detiene, se detiene o se ejecuta lentamente; en todos los casos violando una métrica de disponibilidad.	A4	Vulnerabilidad en el código fuente, que permitía realizar inyección SQL permitiendo al usuario elevar sus privilegios y manipular la información no permitida	Elevación de privilegios, Manipulación	Externo

B47	Secuencias de comandos entre sitios	Aplicación Web	Manipulación	Un agente externo interrumpe el flujo de datos a través de un límite de confianza en cualquier dirección.	A2	El sitio web era obsoleto no usaba https, permitiendo a un usuario malicioso realizar operaciones no permitidas.	Manipulación	Externo
B50	Posible falta de validación de entrada para el navegador / dispositivo móvil	Aplicación Web	Manipulación	Un atacante puede pasar datos al Navegador / Dispositivo móvil para cambiar el flujo de ejecución del programa dentro del Navegador / Dispositivo móvil a elección del atacante.	A3	Vulnerabilidad en el código fuente, que permitía acceder a tokens de acceso sin necesidad de conectarse.	Manipulación, repudio	Externo
					A1	Se utilizó *malware* o *ramsonware*, aprovechando la mala configuración de la red y falta de control de autenticación en el servidor con la base de datos.	Manipulación	Externo

5.2. Evaluación de riesgos

Para evaluar los riesgos del escenario tipo, se utilizarán tanto el catálogo de amenazas, como los perfiles de atacantes, para crear arboles de ataque que permitan cuantificar el riesgo inherente.

5.2.1. Generación de árboles de ataque

En base al catálogo de amenazas usado y a la revisión de literatura con el uso de la herramienta ADTool, se genera el siguiente árbol de ataque para el escenario tipo a usarse. El árbol completo se puede apreciar en el Anexo IV. Para una mejor comprensión este árbol va a ser divido por sus objetivos principales [30] en la Figura 7.

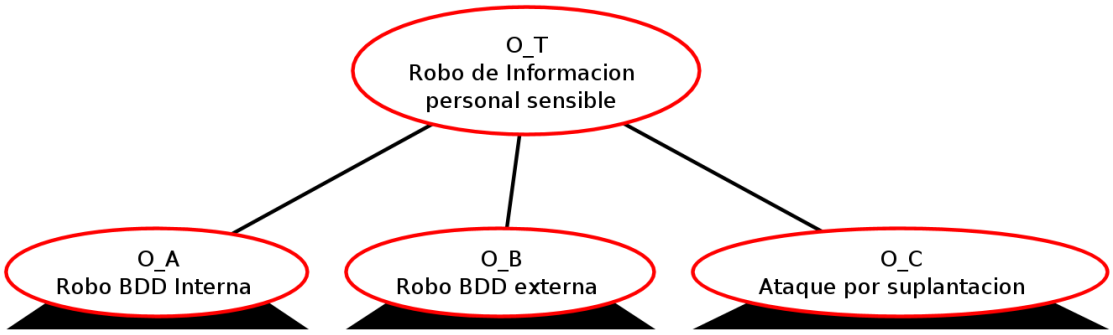


Figura 7 - Árbol de ataque “Robo de información sensible” – Root

En la Figura 8 se observa el nodo O_A del árbol de ataque.

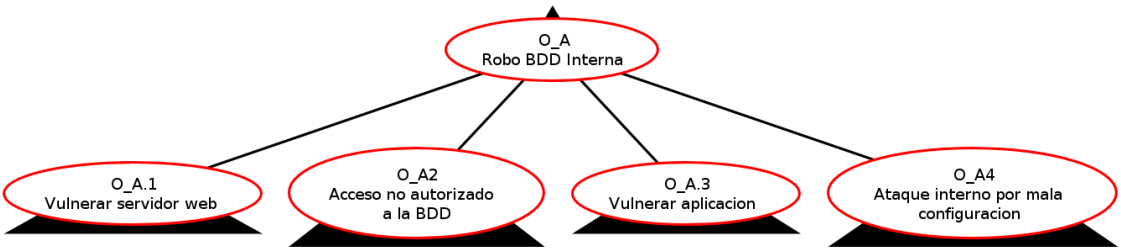


Figura 8 - Árbol de ataque “Robo de información sensible” - Nodo O_A

En la Figura 9 se observa el nodo O_A.1 del árbol de ataque.

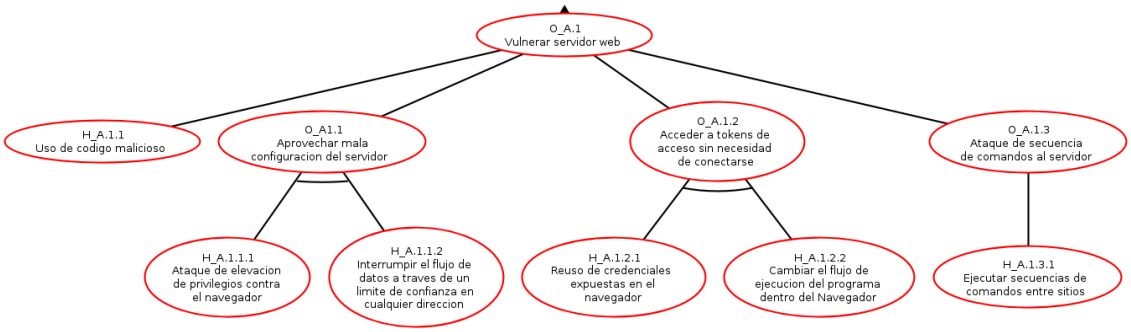


Figura 9 - Árbol de ataque “Robo de información sensible” - Nodo O_A.1

En la Figura 10 se observa el nodo O_A.2 del árbol de ataque.

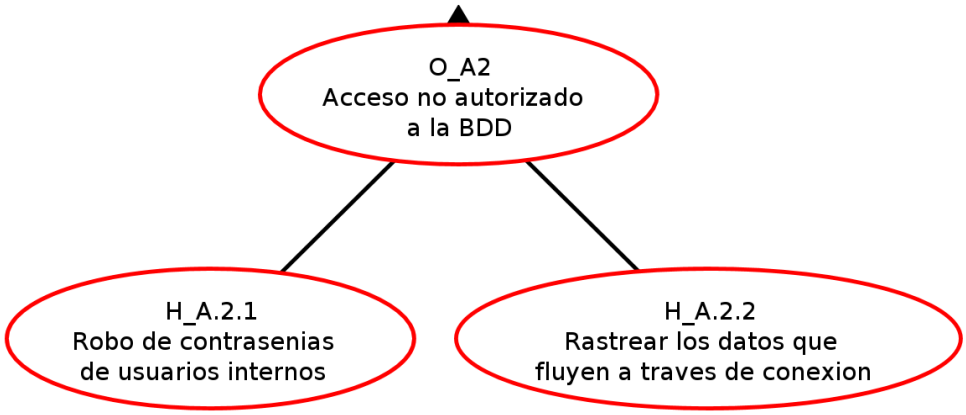


Figura 10 - Árbol de ataque “Robo de información sensible” - Nodo O_A.2

En la Figura 11 se observa el nodo O_A.3 del árbol de ataque.

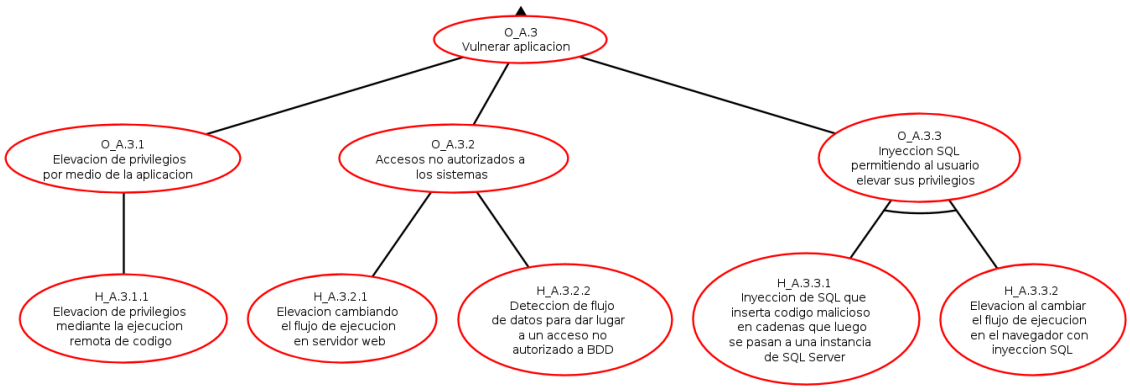


Figura 11 - Árbol de ataque “Robo de información sensible” - Nodo O_A.3

En la Figura 12 se observa el nodo O_A.4 del árbol de ataque.

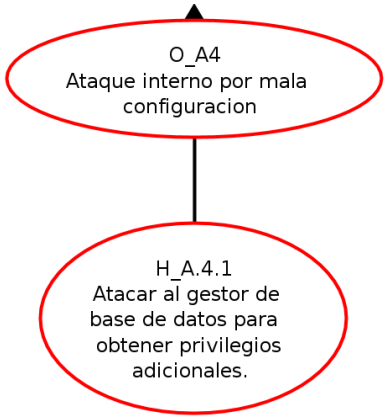


Figura 12 - Árbol de ataque “Robo de información sensible” - Nodo O_A.4

En la Figura 13 se observa el nodo O_B del árbol de ataque.

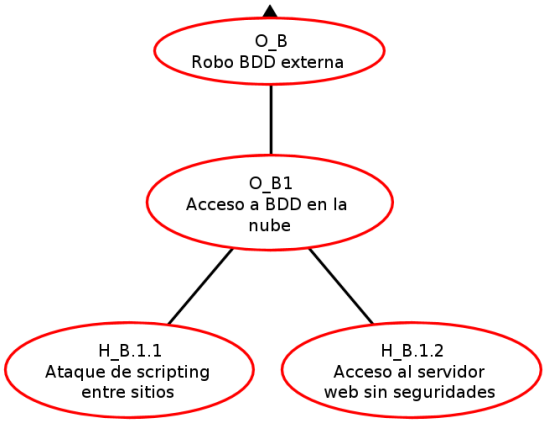


Figura 13 - Árbol de ataque “Robo de información sensible” - Nodo O_B

En la Figura 14 se observa el nodo O_C del árbol de ataque.

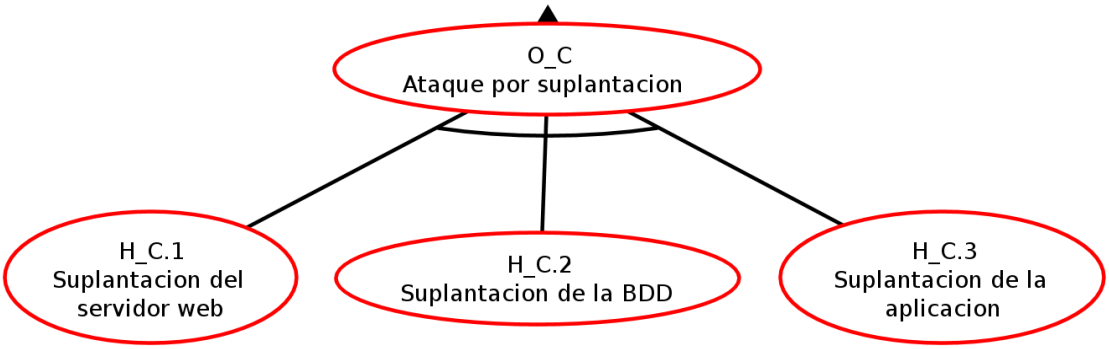


Figura 14 - Árbol de ataque "Robo de información sensible" - Nodo O_C

5.2.2. Definición de atributos y valores para nodos hijos

Como primer paso se procede a detallar los nodos del árbol generado. Con el objetivo de entender el mismo de manera más sencilla se presenta la Tabla 11.

Tabla 11 - Codificación del árbol de ataque "Robo de información sensible"

CÓDIGO	DESCRIPCIÓN	CÓDIGO DE AMENAZA
H_A.1.1	Uso de código malicioso	A1
H_A.1.1.1	Ataque de elevación de privilegios contra el navegador	B43
H_A.1.1.2	Interrumpir el flujo de datos a través de un límite de confianza en cualquier dirección	B47
H_A.1.2.1	Reúso de credenciales expuestas en el navegador	B31
H_A.1.2.2	Cambiar el flujo de ejecución del programa dentro del navegador	B50
H_A.1.3.1	Ejecutar secuencias de comandos entre sitios	B44
H_A.2.1	Robo de contraseñas de usuarios internos	B18
H_A.2.2	Rastrear los datos que fluyen a través de conexión	B30
H_A.3.1.1	Elevación de privilegios mediante la ejecución remota de código	B13
H_A.3.2.1	Elevación cambiando el flujo de ejecución en servidor web	B14
H_A.3.2.2	Detección de flujo de datos para dar lugar a un acceso no autorizado a base de datos	B27
H_A.3.3.1	Inyección de SQL que inserta código malicioso en cadenas que luego se pasan a una instancia de SQL Server para su análisis y ejecución	B16
H_A.3.3.2	Elevación al cambiar el flujo de ejecución en el navegador con inyección SQL	B21
H_A.4.1	Atacar al Gestor de base de datos para obtener privilegios adicionales	B19
H_B.1.1	Ataque de scripting entre sitios	B25
H_B.1.2	Acceso al servidor web sin seguridades	B26
H_C.1	Suplantación del servidor web	B33

CÓDIGO	DESCRIPCIÓN	CÓDIGO DE AMENAZA
H_C.2	Suplantación de la BDD	B35
H_C.3	Suplantación de la aplicación	B39
O_A.1.1	Aprovechar mala configuración del servidor	A2
O_A.1.2	Acceder a tokens de acceso sin necesidad de conectarse	A3
O_A.1.3	Ataque de secuencia de comandos al servidor	A6
O_A.2	Acceso no autorizado a la BDD	A5
O_A.3.1	Elevación de privilegios por medio de la aplicación	A7
O_A.3.2	Accesos no autorizados a los sistemas	A8
O_A.3.3	Inyección SQL permitiendo al usuario elevar sus privilegios	A4
O_A.1	Vulnerar servidor web	
O_A.3	Vulnerar aplicación	
O_A.4	Ataque interno por mala configuración	
O_B.1	Acceso a BDD en la nube	
O_A	Robo BDD interna	
O_B	Robo BDD externa	
O_C	Ataque por suplantación	
O_T	Robo de Información personal sensible	

Los atributos usados en cada uno de los nodos del árbol de ataque serán todos los indicados por la Tabla 3, y los valores asignados están propuestos en base a la búsqueda sistemática de escenarios de brechas. En la Tabla 12 se presentan los valores iniciales para los nodos tipo hoja del árbol de ataque.

Tabla 12 - Valores de atributos iniciales del árbol de ataque “Robo de información sensible”

NODO	ATACANTE	COSTO	IMPACTO	HABILIDAD	PROBABILIDAD	RIESGO
H_A.1.1	Externo	2	7	0.50	0.75	1.3125
H_A.1.1.1	Externo	2	7	1.00	0.80	2.8000
H_A.1.1.2	Externo	2	7	1.00	0.75	2.6250
H_A.1.2.1	Externo	2	8	1.00	0.75	3.0000
H_A.1.2.2	Externo	2	7	1.00	0.75	2.6250
H_A.1.3.1	Externo	2	8	1.00	0.70	2.8000
H_A.2.1	Externo	2	8	1.25	0.50	2.5000
H_A.2.2	Externo	2	7	1.00	0.70	2.4500
H_A.3.1.1	Externo	2	7	1.00	0.60	2.1000
H_A.3.2.1	Externo	2	7	1.00	0.70	2.4500
H_A.3.2.2	Externo	2	8	1.25	0.60	3.0000
H_A.3.3.1	Externo	2	6	1.00	0.80	2.4000
H_A.3.3.2	Externo	2	6	1.00	0.65	1.9500

NODO	ATACANTE	COSTO	IMPACTO	HABILIDAD	PROBABILIDAD	RIESGO
H_A.4.1	Interno	1	8	0.50	0.40	1.6000
H_B.1.1	Externo	2	8	1.00	0.25	1.0000
H_B.1.2	Externo	1	10	1.00	0.75	7.5000
H_C.1	Externo	3	10	1.25	0.25	1.0417
H_C.2	Externo	3	10	1.25	0.20	0.8333
H_C.3	Externo	3	10	1.25	0.40	1.6667

5.2.3. Propagación de valores

Después de asignar valores a los nodos hoja, los atributos se propagan por el árbol hasta que se determinen estos en el nodo superior (*Propagated Up*) [12], esta propagación se realiza por un conjunto de reglas específicas que se indican en la Tabla 13.

Tabla 13 - Fórmulas de propagación de atributos [12]

ATRIBUTO	*AND*	*OR*
Costo	$\sum_{i=1}^{n} costo_i$	$\frac{\sum_{i=1}^{n} prob_1 * costo_i}{\sum_{i=1}^{n} prob_i}$
Impacto	$\frac{10^n - \prod_{i=1}^{n}(10 - impacto_i)}{10^{(n-1)}}$	$Max_{1=1}^{n} impacto_i$
Probabilidad	$\prod_{i=1}^{n} prob_i$	$1 - \prod_{i=1}^{n}(1 - prob_i)$
Habilidad	$Max_{1=1}^{n} Habilidad_i$	$Min_{1=1}^{n} habilidad_i$
prob ∈ $(0,1)$, costo ∈ $(1,2,3)$, impacto ∈ $(1,10)$, $habilidad(0.25,1.25)$, n = # de nodos hijo.		

Con el fin de trabajar con un árbol de ataque más probable, se utilizará el criterio de eliminar todos los nodos que exijan una habilidad muy alta, ya que, al necesitar un elevado esfuerzo técnico, es poco probable que ese ataque se materialice, con esta definición antes de propagar todos los atributos se procede a propagar el atributo habilidad por el árbol de ataque generado.
En la Figura 15 presentada a continuación se puede apreciar gráficamente la propagación el atributo habilidad a través de nodos *AND* ($Max_{1=1}^{n} Habilidad_i$) y nodos *OR* ($Min_{1=1}^{n} habilidad_i$).

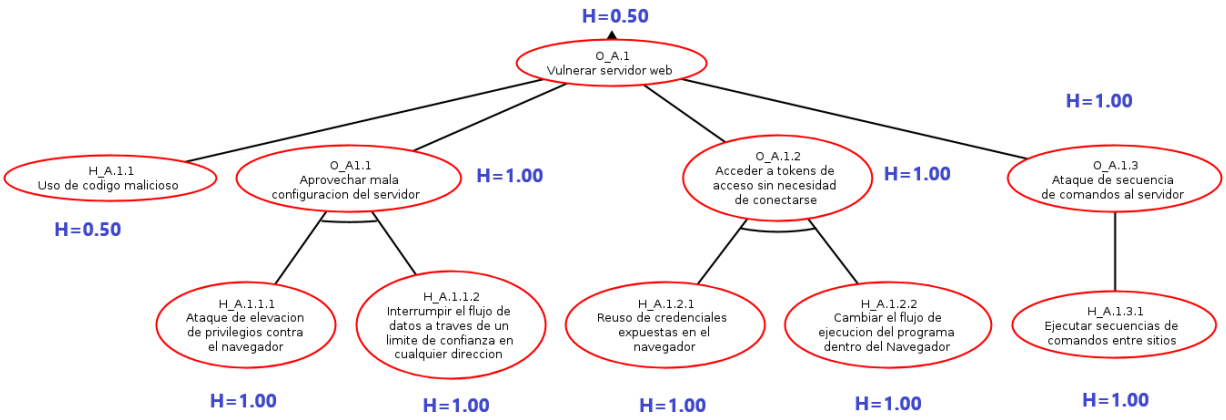


Figura 15 - Propagación del atributo habilidad por el nodo O_A.1

Propagando el atributo Habilidad por todo el árbol de ataque “Robo de Información Sensible” se obtienen los valores de la Tabla 14.

Tabla 14 - Propagación del atributo habilidad

CÓDIGO	HABILIDAD
H_A.1.1	0.50
H_A.1.1.1	1.00
H_A.1.1.2	1.00
H_A.1.2.1	1.00
H_A.1.2.2	1.00
H_A.1.3.1	1.00
H_A.2.1	1.25
H_A.2.2	1.00
H_A.3.1.1	1.00
H_A.3.2.1	1.00
H_A.3.2.2	1.25
H_A.3.3.1	1.00
H_A.3.3.2	1.00
H_A.4.1	0.50
H_B.1.1	1.00
H_B.1.2	1.00
H_C.1	1.25
H_C.2	1.25
H_C.3	1.25
O_A.1.1	1
O_A.1.2	1
O_A.1.3	1

CÓDIGO	HABILIDAD
O_A.2	1
O_A.3.1	1
O_A.3.2	1
O_A.3.3	1
O_A.1	0.5
O_A.3	1
O_A.4	0.5
O_B.1	1
O_A	0.5
O_B	1
O_C	1.25
O_T	0.5

De acuerdo con el criterio establecido, los nodos a eliminar del análisis son: H_A.2.1, H_A.3.2.2, H_C.1, H_C.2, H_C.3, O_C. El árbol resultante se puede apreciar en el Anexo V. En la Figura 16 se puede ver el árbol de ataque y sus objetivos principales.

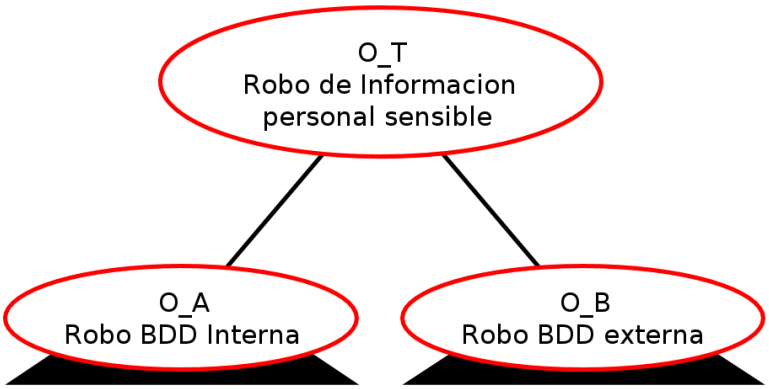


Figura 16 - Árbol de ataque final “Robo de información sensible” – Root

En la Figura 17 se observa el nodo O_A del árbol de ataque final.

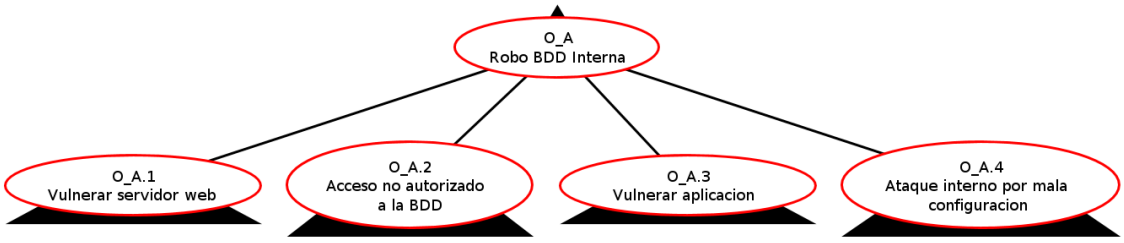


Figura 17 - Árbol de ataque final “Robo de información sensible” - Nodo O_A

En la Figura 18 se observa el nodo O_A.1 del árbol de ataque final.

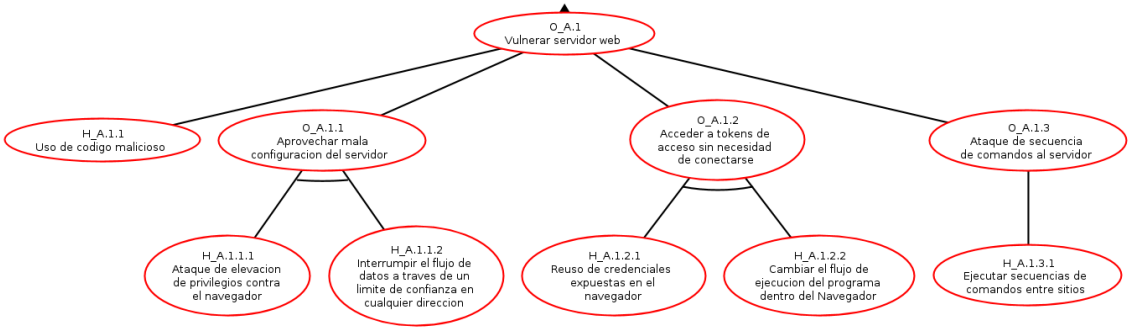


Figura 18 - Árbol de ataque final “Robo de información sensible” - Nodo O_A.1

En la Figura 19 se observa el nodo O_A.2 del árbol de ataque final.

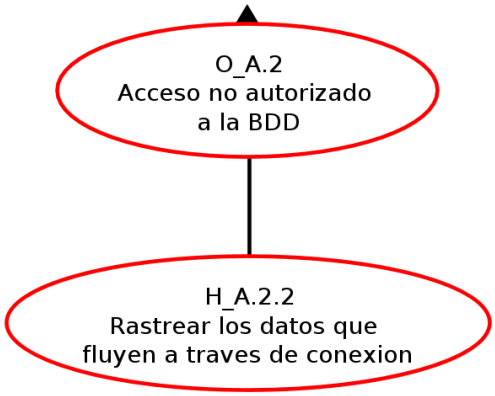


Figura 19 - Árbol de ataque final “Robo de información sensible” - Nodo O_A.2

En la Figura 20 se observa el nodo O_A.3 del árbol de ataque final.

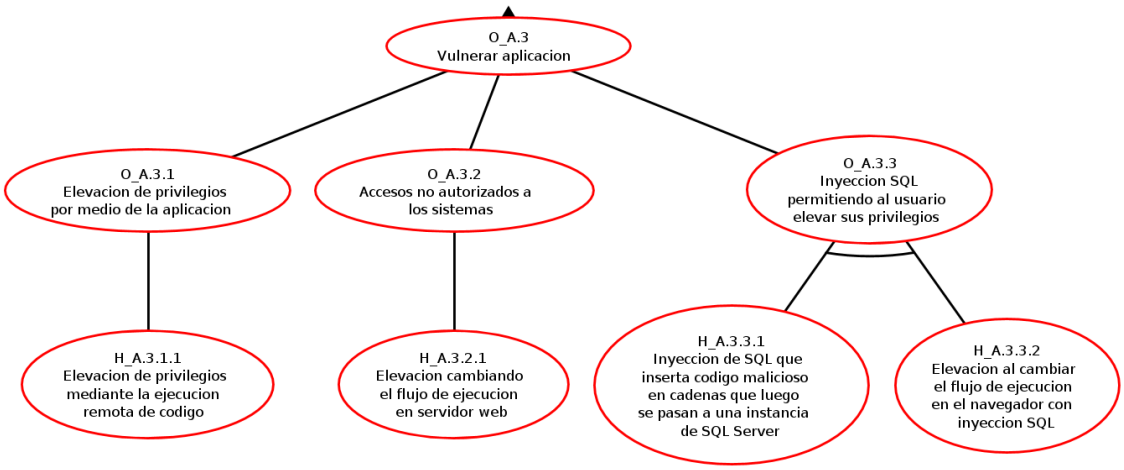


Figura 20 - Árbol de ataque final “Robo de información sensible” - Nodo O_A.3

En la Figura 21 se observa el nodo O_A.4 del árbol de ataque final.

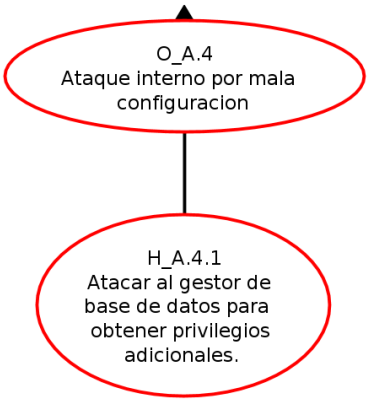


Figura 21 - Árbol de ataque final “Robo de información sensible” - Nodo O_A.4

En la Figura 22 se observa el nodo O_B del árbol de ataque final.

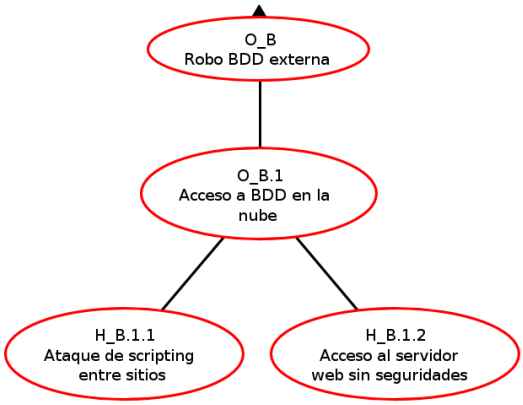


Figura 22 - Árbol de ataque final "Robo de información sensible" - Nodo O_B

Con el árbol de ataque correctamente definido y previo al cálculo del riesgo inherente es necesario propagar los atributos por todos los nodos. Para conseguir este objetivo, se utilizará la codificación de la Tabla 11 y las fórmulas de la Tabla 13 sobre los valores iniciales de la Tabla 12.

En la Tabla 15 se presentan los valores propagados por todo el árbol de ataque.

Tabla 15 - Propagación de atributos por el árbol de ataque "Robo de información sensible"

CÓDIGO	COSTO	IMPACTO	HABILIDAD	PROBABILIDAD	RIESGO
H_A.1.1	2.0000	7.0000	0.5000	0.7500	1.3125
H_A.1.1.1	2.0000	7.0000	1.0000	0.8000	2.8000
H_A.1.1.2	2.0000	7.0000	1.0000	0.7500	2.6250
H_A.1.2.1	2.0000	8.0000	1.0000	0.7500	3.0000
H_A.1.2.2	2.0000	7.0000	1.0000	0.7500	2.6250
H_A.1.3.1	2.0000	8.0000	1.0000	0.7000	2.8000
H_A.2.2	2.0000	7.0000	1.0000	0.7000	2.4500
H_A.3.1.1	2.0000	7.0000	1.0000	0.6000	2.1000
H_A.3.2.1	2.0000	7.0000	1.0000	0.7000	2.4500
H_A.3.3.1	2.0000	6.0000	1.0000	0.8000	2.4000
H_A.3.3.2	2.0000	6.0000	1.0000	0.6500	1.9500
H_A.4.1	1.0000	8.0000	0.5000	0.4000	1.6000
H_B.1.1	2.0000	8.0000	1.0000	0.2500	1.0000
H_B.1.2	1.0000	10.0000	1.0000	0.7500	7.5000
O_A.1.1	4.0000	9.1000	1.0000	0.6000	1.3650
O_A.1.2	4.0000	9.4000	1.0000	0.5625	1.3219
O_A.1.3	2.0000	8.0000	1.0000	0.7000	2.8000
O_A3.1	2.0000	7.0000	1.0000	0.6000	2.1000
O_A3.2	2.0000	7.0000	1.0000	0.7000	2.4500

CÓDIGO	COSTO	IMPACTO	HABILIDAD	PROBABILIDAD	RIESGO
O_A3.3	4.0000	8.4000	1.0000	0.5200	1.0920
O_A.1	2.8900	9.4000	0.5000	0.9869	1.6050
O_A.2	2.0000	7.0000	1.0000	0.7000	2.4500
O_A.3	2.5714	8.4000	1.0000	0.9424	3.0785
O_A.4	1.0000	8.0000	0.5000	0.4000	1.6000
O_B.1	1.2500	10.0000	1.0000	0.8125	6.5000
O_A	2.3357	9.4000	0.5000	0.9999	2.0120
O_B	1.2500	10.0000	1.0000	0.8125	6.5000
OT	1.8489	10.0000	0.5000	1.0000	2.7043

Para entender de manera más clara como se obtienen los valores de los atributos por todo el árbol, se utilizarán los nodos O_A.1.1 y O_B.1 para ejemplificar los cálculos en nodos *AND* y *OR* respectivamente.

Para calcular los valores del nodo O_A.1.1 se deben usar los valores de los nodos O_A.1.1.1 y O_A.1.1.2 con una relación *AND*.

Usando las fórmulas de la Tabla 13, se tiene:

Costo O_A.1.1 = Costo O_A.1.1.1 + Costo O_A.1.1.2

Costo O_A.1.1 = 2 + 2

Costo O_A.1.1 = 4

Impacto O_A.1.1 = $\frac{10^2-\left((10-Impacto\ O\_A.1.1.1)x(10-Impacto\ O\_A.1.1.2)\right)}{10^{(2-1)}}$

Impacto O_A.1.1 = $\frac{100-((10-7)x(10-7))}{10^{(1)}}$

Impacto O_A.1.1 = $\frac{100-(9)}{10^{(1)}}$

Impacto O_A.1.1 = 9.1

Habilidad O_A.1.1 = $Max_{1=1}^{2}(Habilidad\ O\_A.1.1.1 : Habilidad\ O\_A.1.1.2)$

Habilidad O_A.1.1 = $Max\ (1 : 1)$

Habilidad O_A.1.1 = 1

Probabilidad O_A.1.1 = Probabilidad O_A.1.1.1 x Probabilidad O_A.1.1.2

Probabilidad O_A.1.1 = 0.80 * 0.75

Probabilidad O_A.1.1 = 0.60

Riesgo O_A.1.1 = $\frac{(\text{Probabilidad O\_A.1.1 x Impacto O\_A.1.1 x Habilidad O\_A.1.1})}{Costo\ O\_A.1.1}$

Riesgo O_A.1.1 = $\frac{(0.60\ \text{x}\ 9.1\ \text{x}\ 1)}{4}$

Riesgo O_A.1.1 = 1.3650

En Figura 23 se presenta gráficamente los valores calculados sobre un nodo AND.

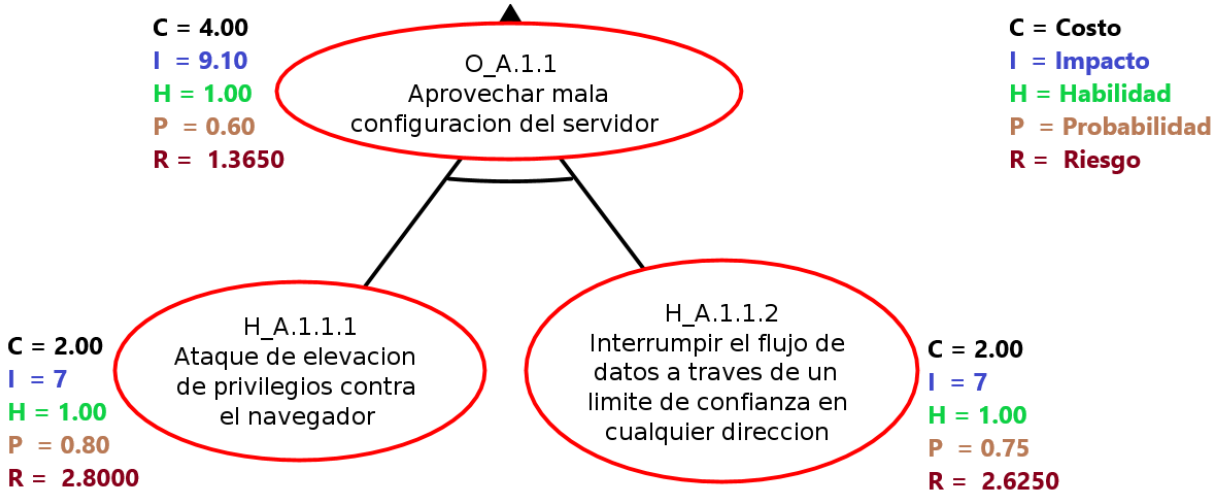


Figura 23 - Cálculo de atributos en nodo AND

Para calcular los valores del nodo O_B.1 se deben usar los valores de los nodos O_B.1.1 y O_B.1.2 con una relación *OR*.

Usando las fórmulas de la Tabla 13, se tiene:

Costo O_B.1 $= \frac{((Probabilidad O\_B.1.1 \; x \; Costo \; O\_B.1.1) + (Probabilidad \; O\_B1.2 \; x \; Costo \; O\_B1.2))}{(Probabilidad \; O\_B.1.1 + Probabilidad \; O\_B.1.2)}$

Costo O_B.1 $= \frac{((0.25 \; x \; 2) + (0.75 \; x \; 1))}{(0.25 + 0.75)}$

Costo O_B.1 $= \frac{((0.50) + (0.75))}{(1)}$

Costo O_B.1 = 1.25

Impacto O_B.1 $= Max \; (Impacto \; O\_B.1.1 : Impacto \; O\_B.1.2)$

Impacto O_B.1 $= Max \; (8 : 10)$

Impacto O_B.1 = 10

Habilidad O_B.1 $= Min \; (Habilidad \; O\_B.1.1 : Habilidad \; O\_B.1.2)$

Habilidad O_B.1 $= Min \; (1 : 1)$

Habilidad O_B.1 $= 1$

Probabilidad O_B.1 = 1-(1-Probabilidad O_B.1.1) x (1-Probabilidad O_B.1.2)

Probabilidad O_B.1 = 1-((1-0.25) x (1-0.75))

Probabilidad O_B.1 = 1-((0.75) x (0.25))

Probabilidad O_B.1 = 1-(0.1875)

Probabilidad O_B.1 = 0.8125

$$\text{Riesgo O\_B.1} = \frac{(\text{Probabilidad O\_B.1 x Impacto O\_B.1 x Habilidad O\_B.1})}{Costo\ O\_B.1}$$

$$\text{Riesgo O\_B.1} = \frac{(0.8125 \text{ x } 10 \text{ x } 1)}{1.25}$$

$$\text{Riesgo O\_B.1} = 6.5000$$

En Figura 24 se presenta gráficamente los valores calculados sobre un nodo OR.

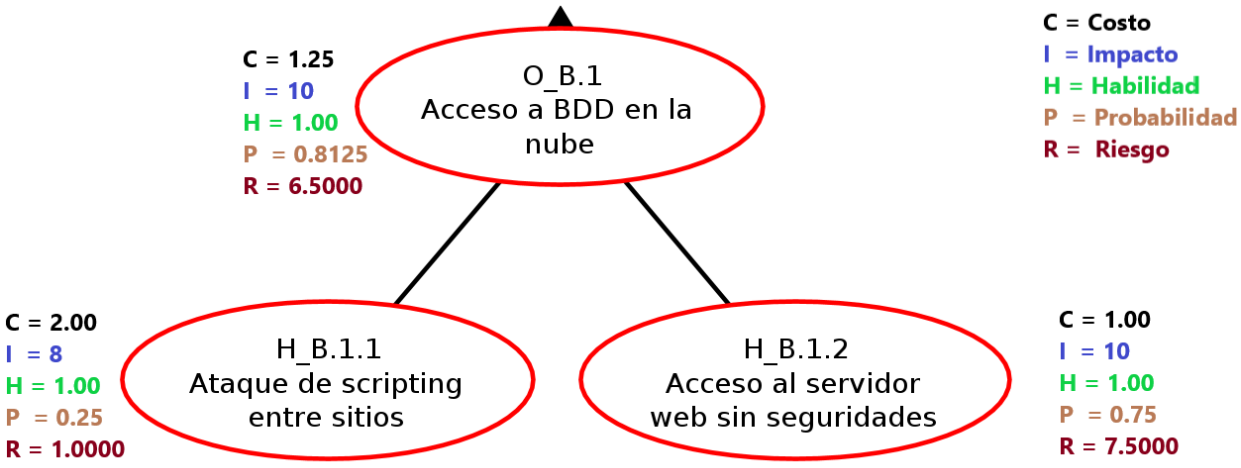


Figura 24 - Cálculo de atributos en nodo OR

5.2.4. Cálculo y valoración del riesgo inherente

Al trabajar los valores de la Tabla 15 en 2 dimensiones, por lado la dimensión impacto, y por otro lado la dimensión compuesta por la probabilidad, la habilidad y el costo, se obtiene la Tabla 16.

Tabla 16 - Riesgo calculado en 2 dimensiones

NODO	PROBABILIDAD * HABILIDAD / COSTO	IMPACTO	RIESGO
H_A.1.1	0.1875	7.0000	1.3125
H_A.1.1.1	0.4000	7.0000	2.8000
H_A.1.1.2	0.3750	7.0000	2.6250
H_A.1.2.1	0.3750	8.0000	3.0000
H_A.1.2.2	0.3750	7.0000	2.6250
H_A.1.3.1	0.3500	8.0000	2.8000
H_A.2.2	0.3500	7.0000	2.4500
H_A.3.1.1	0.3000	7.0000	2.1000
H_A.3.2.1	0.3500	7.0000	2.4500
H_A.3.3.1	0.4000	6.0000	2.4000
H_A.3.3.2	0.3250	6.0000	1.9500

NODO	PROBABILIDAD * HABILIDAD / COSTO	IMPACTO	RIESGO
H_A.4.1	0.2000	8.0000	1.6000
H_B.1.1	0.1250	8.0000	1.0000
H_B.1.2	0.7500	10.0000	7.5000
O_A.1.1	0.1500	9.1000	1.3650
O_A.1.2	0.14063	9.4000	1.3219
O_A.1.3	0.3500	8.0000	2.8000
O_A3.1	0.3000	7.0000	2.1000
O_A3.2	0.3500	7.0000	2.4500
O_A3.3	0.1300	8.4000	1.0920
O_A.1	0.17074	9.4000	1.6050
O_A.2	0.3500	7.0000	2.4500
O_A.3	0.36649	8.4000	3.0785
O_A.4	0.2000	8.0000	1.6000
O_B.1	0.6500	10.0000	6.5000
O_A	0.21405	9.4000	2.0120
O_B	0.6500	10.0000	6.5000
OT	0.27043	10.0000	2.7043

Los valores obtenidos del atributo riesgo de cada nodo corresponden al riesgo inherente, debido a que en el árbol aún no se proponen controles de seguridad para reducir el riesgo. Siendo el riesgo inherente total del árbol, el correspondiente al nodo OT, mismo que posee un valor de 2.7042.

Para realizar un análisis visual de estos valores, siguiendo un método similar al de [5] En la Figura 25 se presenta el mapa semántico para determinar la criticidad de los riesgos registrados.

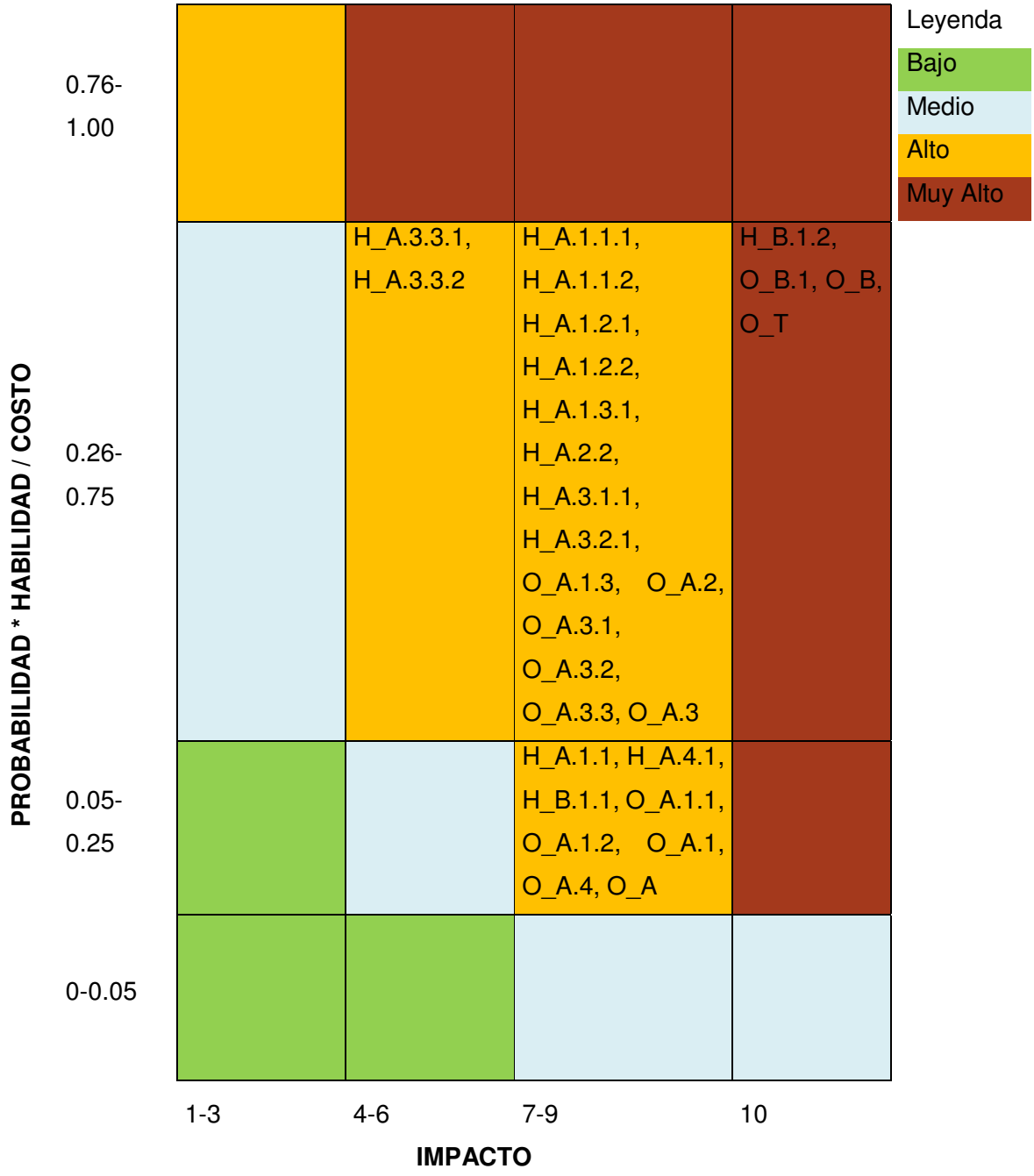


Figura 25 - Mapa semántico de riesgo inherente

Se puede apreciar que todos los riesgos inherentes del árbol de ataque del caso de estudio se encuentran entre Altos y Muy Altos, siendo el riesgo inherente total, muy alto, análisis que coincide con la realidad del estudio realizado y caracterizado en la Tabla 6, en la que en todos los escenarios propuestos se consiguió el objetivo del ataque, que era robar información sensible.

5.3. Control de riesgos

Una etapa fundamental del ciclo de gestión de riesgos propuesto en el presente trabajo es el tratamiento de los riesgos, para la cual es necesario plantear controles de seguridad basados en el EGSI el cual se fundamenta en la norma ISO/EC 27002 que tiene exactamente la misma estructura del Anexo A de la Norma ISO 27001, así, cada control del Anexo A existe en ISO 27002, así como una explicación detallada acerca de cómo implementarlo [2]. También se enfocarán los controles de seguridad propuestos en base a los lineamientos dados por el RGPD, esto debido a que en el caso de estudio seleccionado se utilizan brechas de seguridad que afectan a la información personal sensible de los usuarios de los sistemas de información.
Como se indica en la sección 3 “Propuesta de ciclo de gestión de riesgos” del presente trabajo, la lista de controles de seguridad que se utilizaran para la generación de los árboles de defensa se encuentra en el Anexo II y están basados en EGSI y RGPD y los controles sugeridos por [21].

5.4. Tratamiento de riesgos

Para tratar los riesgos encontrados en la etapa de evaluación, se propone usar arboles de defensa que utilizaran los controles de seguridad generados como contramedidas y con estos calcular el riesgo residual.

5.4.1. Diseño y creación de árboles de defensa

Siguiendo el ciclo de creación de árboles definido en la Figura 6, es necesario definir el tipo de contramedidas que se van a generar en base a los controles propuestos en el Anexo II. Con esta finalidad es indispensable considerar que las contramedidas actúan sobre el riesgo [43]:

- Reduciendo la frecuencia de las amenazas: (preventivas). Las ideales llegan a impedir que la amenaza se materialice.
- Limitando el daño causado: Unas limitan la posible degradación; otras permiten detectar el ataque para frenar que la degradación avance.
- Otras permiten la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las consecuencias se limitan.

Resumiendo lo indicado en el párrafo anterior se pueden implementar contramedidas que actúen sobre:

- La probabilidad de que se materialice una amenaza.

- El impacto causado por la materialización de una amenaza.

En la Tabla 3, se encuentran los atributos usados para la generación de los árboles de ataque, a estos es necesario aumentar los atributos para las contramedidas usadas en los árboles de defensa.
En la Tabla 17 se presentan las contramedidas a usar y sus valore generales

Tabla 17 - Contramedidas y valores generales

ATRIBUTO	DESCRIPCIÓN	VALOR
Costo Contramedida	La cantidad de dinero real necesario para financiar la contramedida.	Barato (B) - 1 Moderado (M) - 2 Costoso (C) - 3
Contramedida de Impacto	Efectividad de una contramedida al minimizar el impacto de una amenaza.	0-1
Contramedida de Probabilidad	La supuesta posibilidad de que la contramedida tendrá éxito.	Improbable (I): por debajo del 5% (0.05). Bajo (B): Entre 5% y 25% (0.05 – 0.25). Medio (M): Entre el 25% y el 75% (0.25 – 0.75). Alto (A): más del 75%. Cierto (C): Cerca del 100% (1).

Definidos los atributos y sus valores generales de las contramedidas, se necesita establecer la estrategia para calcular los valores en cada nodo que implemente una contramedida, con este fin se utilizaran las fórmulas indicada en la Tabla 18.

Tabla 18 - Fórmulas de cálculo de atributos en nodos con contramedida

ATRIBUTO	CÁLCULO	LEYENDA
Impacto [43]	$impacto - \frac{impacto\ x\ \text{efec}}{costoC\ x\ 10}$	impacto = impacto original del ataque. efec = efectividad de la contramedida. costoC = costo de la contramedida.
Probabilidad [30]	$prob\ x\ (1 - (probC/costoC))$	prob = probabilidad ataque original. probC = probabilidad de éxito de la contramedida. costoC = costo de la contramedida.
prob $\in (0,1)$, impacto $\in (1,10)$, efec $\in (0,1)$, probC $\in (0,1)$		

En la Tabla 19 se presentan los valores iniciales para los controles de seguridad definidos en el Anexo II, estos valores consideran como referencia el escenario de brechas.

Tabla 19 - Valores estimados por contramedida

CONTROL DE SEGURIDAD	CÓDIGO CONTRAMEDIDA	TIPO DE CONTRAMEDIDA	VALOR	COSTO	VALOR FINAL
Identificar y Asegurar activos fuera de la organización que contienen datos personales sensibles.	C2	Probabilidad	M 0.50	B 1	0.5
Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	C3	Probabilidad	A 0.80	M 2	0.40
Establecer controles para la protección contra código malicioso.	C4	Probabilidad	A 0.80	B 1	0.80
Establecer reglas de control de acceso.	C5	Probabilidad	M 0.75	B 1	0.75
Establecer políticas de cifrado de almacenamiento de datos.	C6	Impacto	9	M 2	4.5
Gestionar privilegios de usuario.	C7	Probabilidad	M 0.75	B 1	0.75

En la Tabla 20 se presentan las contramedidas sustentadas en los controles de seguridad del Anexo II y su aplicación en los nodos seleccionados.

Tabla 20 - Contramedidas por nodo seleccionado

CÓDIGO NODO	DESCRIPCIÓN NODO	CÓDIGO CONTRAMEDIDA
H_A.1.1	Uso de código malicioso	C4
H_A.1.1.1	Ataque de elevación de privilegios contra el navegador	C7
H_A.1.1.2	Interrumpir el flujo de datos a través de un límite de confianza en cualquier dirección.	C3
H_A.1.2.1	Reúso de credenciales expuestas en el navegador	C3

CÓDIGO NODO	DESCRIPCIÓN NODO	CÓDIGO CONTRAMEDIDA
H_A.1.2.2	Cambiar el flujo de ejecución del programa dentro del Navegador	C3
H_A.1.3.1	Ejecutar secuencias de comandos entre sitios	C3
H_A.2.2	Rastrear los datos que fluyen a través de Conexión	C3
H_A.3.1.1	Elevación de privilegios mediante la ejecución remota de código	C7
H_A.3.2.1	Elevación cambiando el flujo de ejecución en Servidor web	C3
H_A.3.3.1	Inyección de SQL que inserta código malicioso en cadenas que luego se pasan a una instancia de SQL Server para su análisis y ejecución	C3
H_A.3.3.2	Elevación al cambiar el flujo de ejecución en el navegador con inyección SQL	C3
H_A.4.1	Atacar al Gestor de base de datos para obtener privilegios adicionales.	C5
H_B.1.1	Ataque de scripting entre sitios	C3
H_B.1.2	Acceso al servidor web sin seguridades	C2
O_A	Robo BDD interna	C6
O_B	Robo BDD externa	C6
O_T	Robo de Información personal sensible	

5.4.2. Generación de árboles de defensa

En base al árbol de ataque final y a los controles de seguridad definidos. mediante la herramienta ADTool, se genera el correspondiente árbol de defensa [30] mismo que se puede ver de manera total en el Anexo VI.

En la Figura 26 se presenta el árbol de defensa con sus objetivos principales.

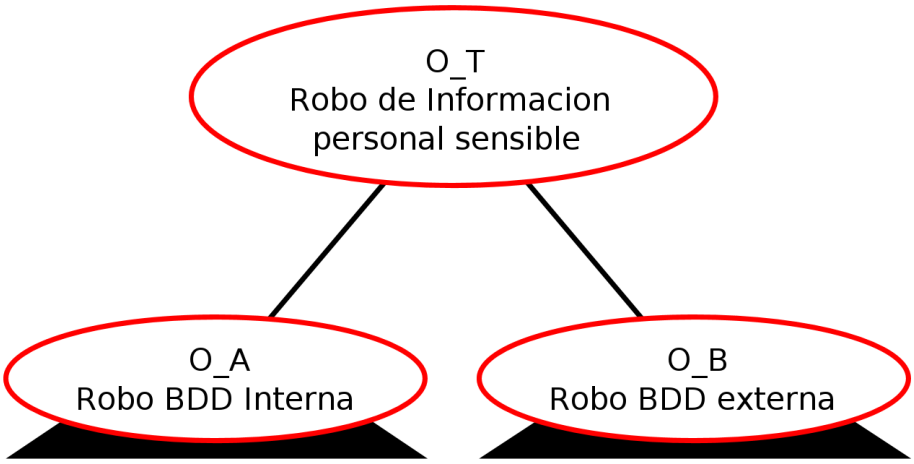


Figura 26 - Árbol de defensa “Robo de información sensible” - Root

En la Figura 27 se observa el nodo O_A del árbol de defensa.

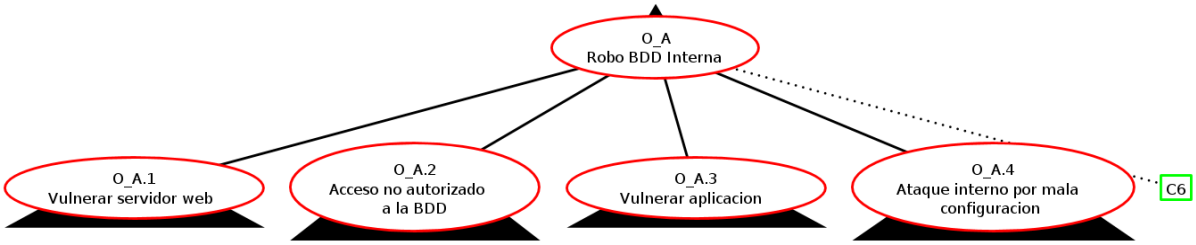


Figura 27 - Árbol de defensa “Robo de información sensible” - Nodo O_A

En la Figura 28 se observa el nodo O_A.1 del árbol de defensa.

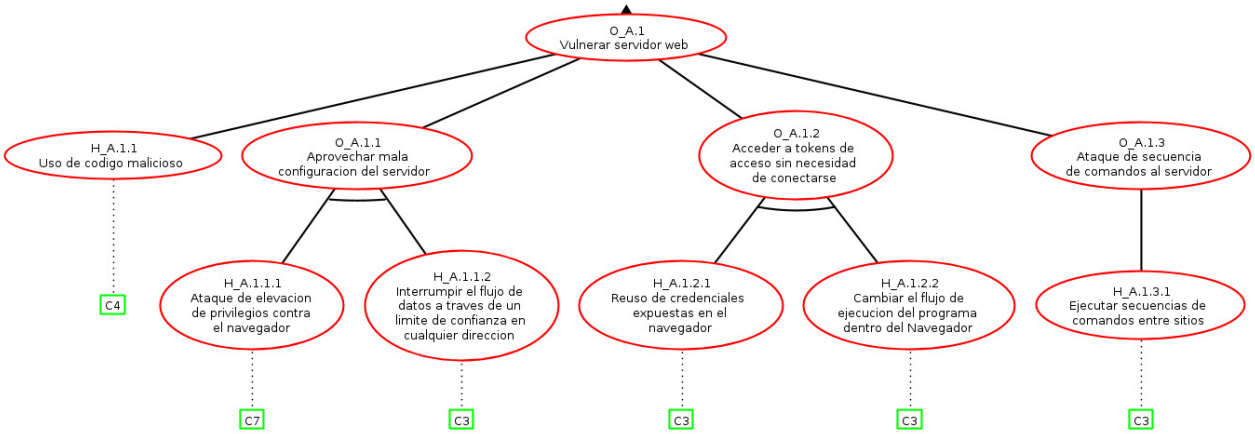


Figura 28 - Árbol de defensa “Robo de información sensible” - Nodo O_A.1

En la Figura 29 se observa el nodo O_A.2 del árbol de defensa.

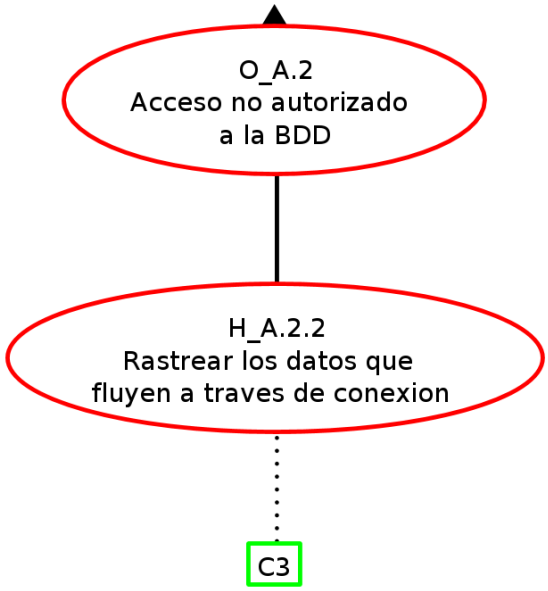


Figura 29 - Árbol de defensa “Robo de información sensible” - Nodo O_A.2

En la Figura 30 se observa el nodo O_A.3 del árbol de defensa.

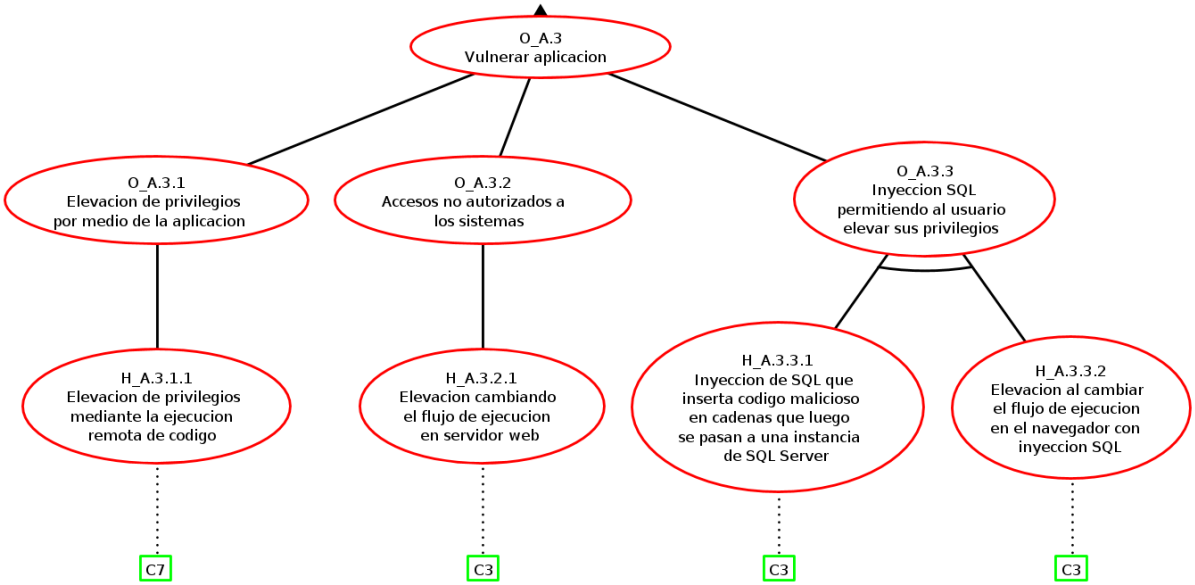


Figura 30 - Árbol de defensa “Robo de información sensible” Nodo O_A.3

En la Figura 31 se observa el nodo O_A.4 del árbol de defensa.

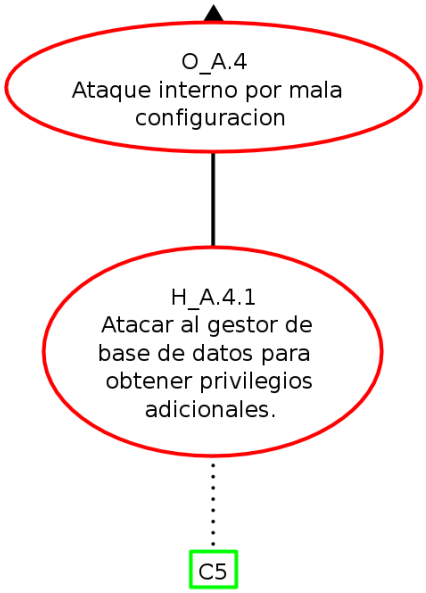


Figura 31 - Árbol de defensa “Robo de información sensible” - Nodo O_A.4

En la Figura 32 se observa el nodo O_B del árbol de defensa.

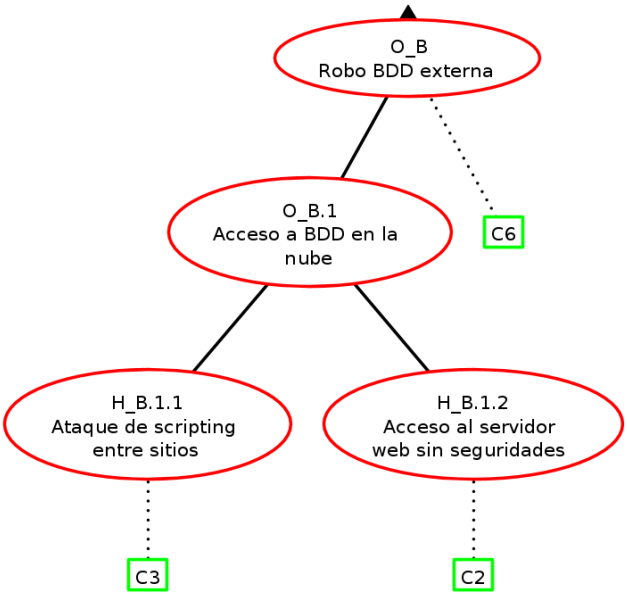


Figura 32 - Árbol de defensa “Robo de información sensible” - Nodo O_B

5.4.3. Definición valores iniciales para nodos hoja usando contramedidas

Usando los valores tipo hoja de la Tabla 15 y los valores de las contramedidas asignados en la Tabla 19, se pueden obtener los valores de los atributos de los nodos tipo hoja del árbol de defensa presentados en la Tabla 21.

Tabla 21 - Valores de atributos iniciales del árbol de defensa “Robo de información sensible”

CÓDIGO	COSTO	IMPACTO	HABILIDAD	PROBABILIDAD	RIESGO	CONTRAMEDIDA	VALOR DE CONTRAMEDIDA	COSTO FINAL	IMPACTO FINAL	HABILIDAD FINAL	PROBABILIDAD FINAL	RIESGO FINAL
H_A.1.1	2.00	7.00	0.50	0.75	1.3125	C4	0.80	2.00	7.00	0.50	0.15	0.2625
H_A.1.1.1	2.00	7.00	1.00	0.80	2.8000	C7	0.75	2.00	7.00	1.00	0.20	0.7000
H_A.1.1.2	2.00	7.00	1.00	0.75	2.6250	C3	0.40	2.00	7.00	1.00	0.45	1.5750
H_A.1.2.1	2.00	8.00	1.00	0.75	3.0000	C3	0.40	2.00	8.00	1.00	0.45	1.8000
H_A.1.2.2	2.00	7.00	1.00	0.75	2.6250	C3	0.40	2.00	7.00	1.00	0.45	1.5750
H_A.1.3.1	2.00	8.00	1.00	0.70	2.8000	C3	0.40	2.00	8.00	1.00	0.42	1.6800
H_A.2.2	2.00	7.00	1.00	0.70	2.4500	C3	0.40	2.00	7.00	1.00	0.42	1.4700
H_A.3.1.1	2.00	7.00	1.00	0.60	2.1000	C7	0.75	2.00	7.00	1.00	0.15	0.5250
H_A.3.2.1	2.00	7.00	1.00	0.70	2.4500	C3	0.40	2.00	7.00	1.00	0.42	1.4700
H_A.3.3.1	2.00	6.00	1.00	0.80	2.4000	C3	0.40	2.00	6.00	1.00	0.48	1.4400
H_A.3.3.2	2.00	6.00	1.00	0.65	1.9500	C3	0.40	2.00	6.00	1.00	0.39	1.1700
H_A.4.1	1.00	8.00	0.50	0.40	1.6000	C5	0.75	1.00	8.00	0.50	0.10	0.4000
H_B.1.1	2.00	8.00	1.00	0.25	1.0000	C3	0.40	2.00	8.00	1.00	0.15	0.6000
H_B.1.2	1.00	10.00	1.00	0.75	7.5000	C2	0.50	1.00	10.00	1.00	0.38	3.7500

Para una mejor compresión de la Tabla 21, se ejemplifica el cálculo de los nuevos valores de atributos para el nodo H_A.1.1

Costo final H_A.1.1 = Costo H_A.1.1

Costo final H_A.1.1 = 2

Impacto final H_A.1.1 = Impacto H_A.1.1 (No existe contramedida de impacto)

Impacto final H_A.1.1 = 7

Habilidad final H_A.1.1 = Habilidad H_A.1.1

Habilidad final H_A.1.1 = 0.50

Probabilidad final H_A.1.1 = Probabilidad H_A.1.1 x (1 – Probabilidad Contramedida C4))

Probabilidad final H_A.1.1 = 0.75 x (1 – 0.80)

Probabilidad final H_A.1.1 = 0.75 x (0.20)

Probabilidad final H_A.1.1 = 0.15

Riesgo final H_A.1.1 = $\frac{(\text{Probabilidad H\_A.1.1x Impacto H\_A.1.1 x Habilidad H\_A.1.1})}{Costo\ \text{H\_A.1.1}}$

Riesgo final H_A.1.1 = $\frac{(0.15 \text{ x } 7 \text{ x } 0.50)}{2}$

Riesgo final H_A.1.1 = 0.2625

5.4.4. Propagación de valores en el árbol de defensa

Previo al cálculo del riesgo residual es necesario propagar los atributos por todos los nodos del árbol de defensa. Para conseguir este objetivo, se utilizarán las fórmulas de la Tabla 13 y Tabla 18, en conjunto con los valores de la Tabla 19 y Tabla 21.

En la Tabla 22 se presentan los valores propagados por el árbol de defensa.

Tabla 22 - Propagación de atributos por el árbol de defensa “Robo de información sensible”

CÓDIGO	COSTO	IMPACTO	HABILIDAD	PROBABILIDAD	RIESGO	CONTRAMEDIDA	VALOR DE CONTRAMEDIDA	COSTO FINAL	IMPACTO FINAL	HABILIDAD FINAL	PROBABILIDAD FINAL	RIESGO FINAL
H_A.1.1	2.0000	7.0000	0.5000	0.7500	1.3125	C4	0.8000	2.0000	7.0000	0.5000	0.1500	0.2625
H_A.1.1.1	2.0000	7.0000	1.0000	0.8000	2.8000	C7	0.7500	2.0000	7.0000	1.0000	0.2000	0.7000
H_A.1.1.2	2.0000	7.0000	1.0000	0.7500	2.6250	C3	0.4000	2.0000	7.0000	1.0000	0.4500	1.5750
H_A.1.2.1	2.0000	8.0000	1.0000	0.7500	3.0000	C3	0.4000	2.0000	8.0000	1.0000	0.4500	1.8000
H_A.1.2.2	2.0000	7.0000	1.0000	0.7500	2.6250	C3	0.4000	2.0000	7.0000	1.0000	0.4500	1.5750
H_A.1.3.1	2.0000	8.0000	1.0000	0.7000	2.8000	C3	0.4000	2.0000	8.0000	1.0000	0.4200	1.6800
H_A.2.2	2.0000	7.0000	1.0000	0.7000	2.4500	C3	0.4000	2.0000	7.0000	1.0000	0.4200	1.4700
H_A.3.1.1	2.0000	7.0000	1.0000	0.6000	2.1000	C7	0.7500	2.0000	7.0000	1.0000	0.1500	0.5250
H_A.3.2.1	2.0000	7.0000	1.0000	0.7000	2.4500	C3	0.4000	2.0000	7.0000	1.0000	0.4200	1.4700
H_A.3.3.1	2.0000	6.0000	1.0000	0.8000	2.4000	C3	0.4000	2.0000	6.0000	1.0000	0.4800	1.4400
H_A.3.3.2	2.0000	6.0000	1.0000	0.6500	1.9500	C3	0.4000	2.0000	6.0000	1.0000	0.3900	1.1700
H_A.4.1	1.0000	8.0000	0.5000	0.4000	1.6000	C5	0.7500	1.0000	8.0000	0.5000	0.1000	0.4000
H_B.1.1	2.0000	8.0000	1.0000	0.2500	1.0000	C3	0.4000	2.0000	8.0000	1.0000	0.1500	0.6000
H_B.1.2	1.0000	10.0000	1.0000	0.7500	7.5000	C2	0.5000	1.0000	10.0000	1.0000	0.3750	3.7500
O_A.1.1	4.0000	9.1000	1.0000	0.6000	1.3650	-	-	4.0000	9.1000	1.0000	0.0900	0.2048
O_A.1.2	4.0000	9.4000	1.0000	0.5625	1.3219	-	-	4.0000	9.4000	1.0000	0.2025	0.4759
O_A.1.3	2.0000	8.0000	1.0000	0.7000	2.8000	-	-	2.0000	8.0000	1.0000	0.4200	1.6800
O_A3.1	2.0000	7.0000	1.0000	0.6000	2.1000	-	-	2.0000	7.0000	1.0000	0.1500	0.5250
O_A3.2	2.0000	7.0000	1.0000	0.7000	2.4500	-	-	2.0000	7.0000	1.0000	0.4200	1.4700
O_A3.3	4.0000	8.4000	1.0000	0.5200	1.0920	-	-	4.0000	8.4000	1.0000	0.1872	0.3931
O_A.1	2.8900	9.4000	0.5000	0.9869	1.6050	-	-	2.6348	9.4000	0.5000	0.6422	1.1456
O_A.2	2.0000	7.0000	1.0000	0.7000	2.4500	-	-	2.0000	7.0000	1.0000	0.4200	1.4700
O_A.3	2.5714	8.4000	1.0000	0.9424	3.0785	-	-	2.4945	8.4000	1.0000	0.5993	2.0181
O_A.4	1.0000	8.0000	0.5000	0.4000	1.6000	-	-	1.0000	8.0000	0.5000	0.1000	0.4000
O_B.1	1.2500	10.0000	1.0000	0.8125	6.5000	-	-	1.2857	10.0000	1.0000	0.4688	3.6458
O_A	2.3357	9.4000	0.5000	0.9999	2.0120	C6	4.5000	2.3429	5.1700	0.5000	0.9252	1.0208
O_B	1.2500	10.0000	1.0000	0.8125	6.5000	C6	4.5000	1.2857	5.5000	1.0000	0.4688	2.0052
OT	1.8489	10.0000	0.5000	1.0000	2.7043	-	-	1.9874	5.5000	0.5000	0.9602	1.3287

5.4.5. Cálculo y valoración del riesgo residual

Al trabajar los valores de la Tabla 22 en 2 dimensiones, por lado la dimensión impacto, y por otro lado la dimensión compuesta por la probabilidad, la habilidad y el costo, se obtiene la Tabla 23.

Tabla 23 - Riesgo calculado en 2 dimensiones para el árbol de defensa "Robo de información sensible

NODO	PROBABILIDAD * HABILIDAD / COSTO	IMPACTO	RIESGO
H_A.1.1	0.0375	7.0000	0.2625
H_A.1.1.1	0.1000	7.0000	0.7000
H_A.1.1.2	0.2250	7.0000	1.5750
H_A.1.2.1	0.2250	8.0000	1.8000
H_A.1.2.2	0.2250	7.0000	1.5750
H_A.1.3.1	0.2100	8.0000	1.6800
H_A.2.2	0.2100	7.0000	1.4700
H_A.3.1.1	0.0750	7.0000	0.5250
H_A.3.2.1	0.2100	7.0000	1.4700
H_A.3.3.1	0.2400	6.0000	1.4400
H_A.3.3.2	0.1950	6.0000	1.1700
H_A.4.1	0.0500	8.0000	0.4000
H_B.1.1	0.0750	8.0000	0.6000
H_B.1.2	0.3750	10.0000	3.7500
O_A.1.1	0.0225	9.1000	0.2048
O_A.1.2	0.0506	9.4000	0.4759
O_A.1.3	0.2100	8.0000	1.6800
O_A3.1	0.0750	7.0000	0.5250
O_A3.2	0.2100	7.0000	1.4700
O_A3.3	0.0468	8.4000	0.3931
O_A.1	0.1219	9.4000	1.1456
O_A.2	0.2100	7.0000	1.4700
O_A.3	0.2402	8.4000	2.0181
O_A.4	0.0500	8.0000	0.4000
O_B.1	0.3646	10.0000	3.6458
O_A	0.1974	5.1700	1.0208
O_B	0.3646	5.5000	2.0052
OT	0.2416	5.5000	1.3287

Los valores obtenidos del atributo riesgo de cada nodo corresponden al riesgo residual, debido a que el árbol ya considera controles de seguridad basados que buscan proteger la información

sensible para reducir el riesgo. Siendo el riesgo residual total del árbol, el correspondiente al nodo OT, mismo que posee un valor de 1.49.

Para realizar un análisis visual de estos valores, siguiendo un método similar al de [5] En la Figura 33, se presenta el mapa semántico para determinar la criticidad de los riesgos registrados.

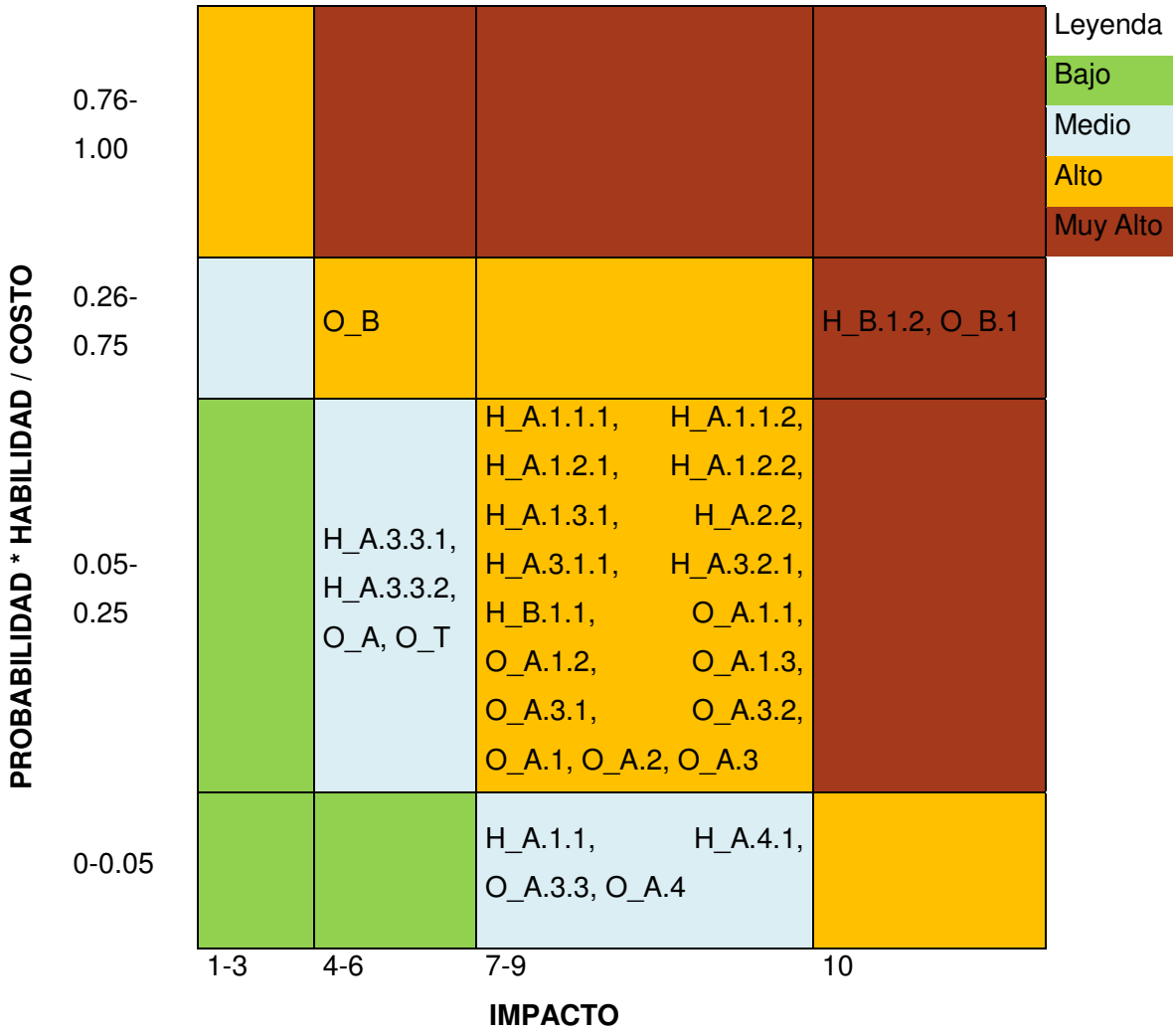


Figura 33 - Mapa semántico de riesgo residual

Una vez aplicados los controles de seguridad propuestos, Se puede apreciar que todos los riesgos residuales del árbol de defensa del caso de estudio, se han minimizado considerablemente, sin embargo aún se tienen riesgos muy altos y altos, pero se puede ver que un porcentaje considerable de riesgos han perdido impacto al bajar a las escalas Media y Baja, es destacable el hecho de que el riesgo residual total ya no es Muy Alto sino Medio, con un impacto reducido casi a la mitad gracias a las contramedidas consideradas.

5.5. Comunicación y validación

Para validar y realizar la comunicación dentro del ciclo es necesario comparar los riesgos: inherente y residual, con esto se puede analizar la efectividad de los controles propuestos.

5.5.1 Comparación entre riesgos

El análisis cualitativo de los mapas semánticos utilizados en las figuras 25 y 33, permite apreciar que la implantación de controles de seguridad reduce considerablemente el riesgo de un sistema de información al ser vulnerado cuando es objeto de un robo de información de datos personales sensibles.

Es importante destacar que luego de implementar controles enfocados a asegurar la privacidad de la información, todos los riegos se vieron controlados en gran medida, permitiendo realizar una gestión adecuada de las vulnerabilidades presentadas.

Para completar el análisis cualitativo realizado, es necesario realizar un análisis de índole cuantitativa, y con este fin, apoyado en el trabajo de [5] se utilizará una variante de la ficha de informes de riesgos, que permitan comparar los riesgos residuales e inherentes para el presente caso de estudio.

En la Tabla 24 se presenta la ficha comparativa de riesgos inherente y residual.

Tabla 24 - Ficha comparativa de riesgos inherente y residual

				RIESGO INHERENTE			RIESGO RESIDUAL			
Código Riesgo	**Descripción del Riesgo**	**Descripción Control**	**Tipo Control**	**Probabilidad**	**Impacto**	**Riesgo**	**Probabilidad**	**Impacto**	**Riesgo**	**% Reducción**
H_A.1.1	Uso de código malicioso	Establecer controles para la protección contra código malicioso.	Probabilidad	0.1875	7.0000	1.3125	0.0375	7.0000	0.2625	80.00
H_A.1.1.1	Ataque de elevación de privilegios contra el navegador	Gestionar privilegios de usuario.	Probabilidad	0.4000	7.0000	2.8000	0.1000	7.0000	0.7000	75.00
H_A.1.1.2	Interrumpir el flujo de datos a través de un límite de confianza en cualquier dirección.	Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	Probabilidad	0.3750	7.0000	2.6250	0.2250	7.0000	1.5750	40.00
H_A.1.2.1	Reúso de credenciales expuestas en el navegador	Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	Probabilidad	0.3750	8.0000	3.0000	0.2250	8.0000	1.8000	40.00
H_A.1.2.2	Cambiar el flujo de ejecución del programa dentro del Navegador	Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	Probabilidad	0.3750	7.0000	2.6250	0.2250	7.0000	1.5750	40.00

				RIESGO INHERENTE			RIESGO RESIDUAL			
Código Riesgo	**Descripción del Riesgo**	**Descripción Control**	**Tipo Control**	**Probabilidad**	**Impacto**	**Riesgo**	**Probabilidad**	**Impacto**	**Riesgo**	**% Reducción**
H_A.1.3.1	Ejecutar secuencias de comandos entre sitios	Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	Probabilidad	0.3500	8.0000	2.8000	0.2100	8.0000	1.6800	40.00
H_A.2.2	Rastrear los datos que fluyen a través de Conexión	Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	Probabilidad	0.3500	7.0000	2.4500	0.2100	7.0000	1.4700	40.00
H_A.3.1.1	Elevación de privilegios mediante la ejecución remota de código	Gestionar privilegios de usuario.	Probabilidad	0.3000	7.0000	2.1000	0.0750	7.0000	0.5250	75.00
H_A.3.2.1	Elevación cambiando el flujo de ejecución en Servidor web	Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	Probabilidad	0.3500	7.0000	2.4500	0.2100	7.0000	1.4700	40.00
H_A.3.3.1	Inyección de SQL que inserta código malicioso en cadenas que	Establecer estándares de configuración segura, desarrollo y	Probabilidad	0.4000	6.0000	2.4000	0.2400	6.0000	1.4400	40.00

				RIESGO INHERENTE			RIESGO RESIDUAL			
Código Riesgo	**Descripción del Riesgo**	**Descripción Control**	**Tipo Control**	**Probabilidad**	**Impacto**	**Riesgo**	**Probabilidad**	**Impacto**	**Riesgo**	**% Reducción**
	luego se pasan a una instancia de SQL Server para su análisis y ejecución	actualización de los sistemas.								
H_A.3.3.2	Elevación al cambiar el flujo de ejecución en el navegador con inyección SQL	Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	Probabilidad	0.3250	6.0000	1.9500	0.1950	6.0000	1.1700	40.00
H_A.4.1	Atacar al Gestor de base de datos para obtener privilegios adicionales.	Establecer reglas de control de acceso.	Probabilidad	0.2000	8.0000	1.6000	0.0500	8.0000	0.4000	75.00
H_B.1.1	Ataque de scripting entre sitios	Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	Probabilidad	0.1250	8.0000	1.0000	0.0750	8.0000	0.6000	40.00
H_B.1.2	Acceso al servidor web sin seguridades	Identificar y Asegurar activos fuera de la organización	Probabilidad	0.7500	10.0000	7.5000	0.3750	10.0000	3.7500	50.00

				RIESGO INHERENTE			RIESGO RESIDUAL			
Código Riesgo	**Descripción del Riesgo**	**Descripción Control**	**Tipo Control**	**Probabilidad**	**Impacto**	**Riesgo**	**Probabilidad**	**Impacto**	**Riesgo**	**% Reducción**
		que contienen datos personales sensibles.								
O_A1.1	Aprovechar mala configuración del servidor			0.1500	9.1000	1.3650	0.0225	9.1000	0.2048	85.00
O_A1.2	Acceder a tokens de acceso sin necesidad de conectarse			0.14063	9.4000	1.3219	0.0506	9.4000	0.4759	64.00
O_A1.3	Ataque de secuencia de comandos al servidor			0.3500	8.0000	2.8000	0.2100	8.0000	1.6800	40.00
O_A.3.1	Elevación de privilegios por medio de la aplicación			0.3000	7.0000	2.1000	0.0750	7.0000	0.5250	75.00
O_A.3.2	Accesos no autorizados a los sistemas			0.3500	7.0000	2.4500	0.2100	7.0000	1.4700	40.00
O_A3.3	Inyección SQL permitiendo al usuario elevar sus privilegios			0.1300	8.4000	1.0920	0.0468	8.4000	0.3931	64.00
O_A.1	Vulnerar servidor web			0.17074	9.4000	1.6050	0.1219	9.4000	1.1456	28.62

				RIESGO INHERENTE			RIESGO RESIDUAL			
Código Riesgo	**Descripción del Riesgo**	**Descripción Control**	**Tipo Control**	**Probabilidad**	**Impacto**	**Riesgo**	**Probabilidad**	**Impacto**	**Riesgo**	**% Reducción**
O_A.2	Acceso no autorizado a la BDD			0.3500	7.0000	2.4500	0.2100	7.0000	1.4700	40.00
O_A.3	Vulnerar aplicación			0.36649	8.4000	3.0785	0.2402	8.4000	2.0181	34.45
O_A.4	Ataque interno por mala configuración			0.2000	8.0000	1.6000	0.0500	8.0000	0.4000	75.00
O_B.1	Acceso a BDD en la nube			0.6500	10.0000	6.5000	0.3646	10.0000	3.6458	43.91
O_A	Robo BDD interna	Establecer políticas de cifrado de almacenamiento de datos.	Impacto	0.21405	9.4000	2.0120	0.1974	5.1700	1.0208	49.27
O_B	Robo BDD externa	Establecer políticas de cifrado de almacenamiento de datos.	Impacto	0.6500	10.0000	6.5000	0.3646	5.5000	2.0052	69.15
O_T	Robo de Información personal sensible			0.27043	10.0000	2.7043	0.2416	5.5000	1.3287	50.86

5.5.2 Análisis de efectividad

En base al trabajo realizado en la ficha comparativa de riesgos inherente y residual se puede aprecia que:

- El riesgo inherente generado por ataques que roban información personal sensible tiene un impacto muy alto, que afecta considerablemente la privacidad de los usuarios de los sistemas de información afectados por este tipo de brechas.
- Los controles de seguridad orientados a salvaguardar la privacidad de la información ayudan a reducir significativamente el impacto de los ataques a los datos personales sensibles, este hecho se evidencia al revisar los riesgos reportados en la ficha comparativa, siendo considerable la reducción del impacto del objetivo total del ataque de 10 a 5.5. Es significativo indicar que aún con controles como la encriptación los datos personales sensibles, siempre se pueden perder datos importantes que afecten a los usuarios de los sistemas.

Con el uso de los mapas semánticos se apreció una reducción de riesgo conservadora, sin embargo, mediante la comparación cuantitativa se puede observar que la reducción del riesgo varía entre el 28 y 85% en todos los riesgos que tienen implementados una contramedida basada en la protección de los datos sensibles personales.

Es importante indicar que pese a tratarse de la primera iteración del ciclo de gestión de riesgos se han obtenido resultados satisfactorios.

5.6. Monitoreo

Considerando los valores de reducción evidenciados en la “Ficha comparativa de riesgos inherente y residual”, se puede declarar de manera categórica que la implementación controles de seguridad basados en EGSI y RGPD para la protección de la privacidad de datos personales sensibles tienen un fuerte y positivo impacto en la gestión de riesgos de los sistemas de información. Y para efectos del presente estudio se puede aceptar el riego y finalizar el ciclo de gestión de riesgos.

De tratarse de un caso de estudio real en la práctica se debería realizar una evaluación de contexto cada cierto periodo como recomienda la norma ISO 27005, esto con la finalidad de poder manejar de manera adecuada los riesgos.

6. CONCLUSIONES Y RECOMENDACIONES

En el caso de estudio de capítulo 5 se pudo demostrar que el ciclo de gestión de riesgos propuesto trabaja de manera adecuada y cumple su cometido en infraestructuras corporativas.

En el Anexo VII se realiza una evaluación del ciclo de gestión propuesto dentro de una tecnología emergente, como lo es el "Internet de la Cosas". En esta evaluación, se puede apreciar que el ciclo trabaja de manera correcta.

La guía simple de implementación del ciclo de gestión propuesta se encuentra en el anexo VIII.

6.1. Conclusiones

- Respondiendo a la pregunta de investigación, se puede concluir que es perfectamente viable integrar dentro del ciclo de gestión de riesgos el uso de controles de seguridad ISO/IEC 27002 con el usa de EGSI y el RGPD.
- En base a los casos de estudio realizados, se puede concluir que se ha propuesto de manera acertada un ciclo de gestión de riesgos, el mismo que utiliza modelado de amenazas automatizado, así como controles de seguridad enfocados en la privacidad, según los lineamientos dados por EGSI, RGPD y la norma ISO/IEC 27002.
- Considerando los casos de estudio trabajados y mediante el uso la revisión sistemática de literatura se puede concluir que es factible definir un escenario de ataque, mismo que considera amenazas comunes a la seguridad y privacidad de la información.
- El uso de árboles de ataque y defensa, constituyen una herramienta valiosa al momento de analizar los riesgos inherentes y residuales de un escenario de amenazas.
- El ciclo de gestión propuesto usa de manera adecuada y consistente las norma ISO 27002, el EGSI y el RGPD, ya que la etapa de control de riesgos se fundamenta en estos ítems, y el esquema general del ciclo está sustentado en la norma ISO 27005.
- Se puede concluir que al implementarse de manera adecuada los controles de seguridad enfocados en la privacidad de datos personales sensibles, se puede reducir de manera considerable los riesgos a los que están sometidos los sistemas de información.

- En tecnologías emergentes se puede apreciar que los controles de seguridad basados en la privacidad son insuficientes, es necesario combinarlos con más controles de seguridad enfocados a las demás dimensiones de la seguridad de la información.

6.2. Recomendaciones

- Se recomienda que en futuros trabajos se incluyan controles que afecten las demás dimensiones de la seguridad de información, como confidencialidad, integridad y disponibilidad, con el fin de ver como estos interactúan con los controles de seguridad enfocados en la privacidad.
- En escenarios reales, se recomiendo realizar más de una sola iteración del ciclo de gestión de riesgos.
- Se recomienda, en el caso de implementaciones reales, realizar periódicamente revisiones de las amenazas a las que está expuesta una organización, usando el ciclo de gestión propuesto.

REFERENCIAS BIBLIOGRÁFICAS

[1] R. R. Coello Yagual y L. M. Pico Versoza, «Análisis de las ventajas y desventajas del sistema de gestión de la seguridad de la información y su influencia en la competitividad de las empresas que utilizan Cloud Computing y Big Data en el Ecuador», INNOVA Res. J., vol. 3, n.o 4, pp. 181-195, 2018.

[2] ISO27000.ES (2019, JUN 13). [Online]. Available: https://www.iso27000.es/sgsi.html.

[3] El Comercio (2019, ABR 16). [Online]. Available: https://www.elcomercio.com/actualidad/hackers-ofensiva-global-ataque-ecuador.html.

[4] Plan V (2019, SEP 16). [Online]. Available: https://www.planv.com.ec/historias/sociedad/la-peor-filtracion-datos-la-historia-del-ecuador-al-descubierto.

[5] M. Rodríguez, C. Piñeiro; P. de Llano, «Mapa de riesgos: Identificación y gestión de riesgos» de: "Atlantic Review of Economics", Colegio de Economistas de A Coruña, A Coruña, 2013.

[6] C. Everett, «A risky business: ISO 31000 and 27005 unwrapped», Comput. Fraud Secur., vol. 2011, n.o 2, pp. 5-7, 2011.

[7] NIST, «NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations», NIST SP-800-53 Ar4, p. 400+, 2013.

[8] Secretaría Nacional de la Administración Pública, «Acuerdo Ministerial 166. Esquema Gubernamental de Seguridad de la Información». Registro Oficial Suplemento 88, 2013.

[9] General Data Protection Regulation. (2016). Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos 167 personales y a la libre circulación de estos datos y por el que se deroga la D Directiva 95/46/CE (Reglamento general de protección de datos). Diario Oficial de La Unión Europea, 2014(119), 1–88. https://doi.org/10.1016/j.yhbeh.2005.02.009

[10] Magerit versión 2, «Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas», vol. 2006, 2012.

[11] R. Pompon, «IT Security Risk Control Management: An Audit Preparation Plan». APRESS, pp. 23-28, 2016.

[12] K. S. Edge, G. C. Dalton, R. A. Raines, y R. F. Mills, «Using attack and protection trees to analyze threats and defenses to homeland security», Proc. - IEEE Mil. Commun. Conf. MILCOM, pp. 1-7, 2006.

[13] T. Sonderen, «A Manual for Attack Trees», p. 81, 2019.

[14] V. Agrawal, "A Framework for the Information Classification in ISO 27005 Standard," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, 2017, pp. 264-269.
[15] M. J. Ramírez, «Estado del arte», Universidad de los Andes, p. 11, 2016.
[16] J. Pino, «Marco de Referencia para la implementación de un esquema gubernamental de seguridad de la información (EGSI), basado en la norma técnica ecuatoriana ISO/IEC 27001:2010 y en concordancia con el acuerdo 166», Quito: Universidad de la Américas, 2014.
[17] C. Cáceres y C. Mena, «Elaboración de la guía de implantación de las normas prioritarias del esquema gubernamental de seguridad de la información EGSI en las entidades de la administración pública central». Escuela Politécnica Nacional, p. 209, 2015.
[18] A. Pinto, «Análisis y planteamiento de políticas de acuerdo con el esquema gubernamental de seguridad de la información (EGSI) para la empresa pública Yachay». Universidad Técnica del Norte, p. 160, 2016.
[19] H. F. Gualotuña Guato y M. G. Quilumbaqui Muenala, «Aplicación de las normas técnicas ISO/IEC 27001 e ISO/IEC 27002 para el cumplimiento del esquema gubernamental de seguridad de la información (EGSI) en la infraestructura del sistema nacional de nivelación y admisión (SNNA)», Escuela Politécnica Nacional, p. 121, 2016.
[20] C. Muyón, T. Guarda, G. Vargas, y G. Ninahualpa, «Esquema Gubernamental de Seguridad de la Información EGSI y su aplicación en las entidades públicas del Ecuador TT», Rev. Ibérica Sistemas. Y Tecnologías de la Información N.18, p. 9, 2018.
[21] A. Yánez, «Propuesta de controles de seguridad de la información desde el enfoque de protección de datos personales para los entes gubernamentales del Ecuador que tienen implementado la estrategia de gobierno en línea», Universidad Espíritu Santo, p. 35, 2018.
[22] M. Gallardo, «Elaboración de una política de seguridad de la información para una institución pública basado en el esquema gubernamental de seguridad de la información», Universidad Internacional SEK, p. 107, 2018.
[23] C. López, «Gobierno De TI Basado En El Esquema Gubernamental De Seguridad De La Información (EGSI) En El Hospital San Luis De Otavalo», Universidad Técnica del Norte, p. 242, 2019.
[24] A. Zambrano, M. Jessica, P. Joselin y L. Sebastiana, «La protección de datos personales: análisis de las leyes en el Ecuador», Escuela Superior Politécnica Agropecuaria de Manabí “Manuel Félix López”, p. 8, 2019.
[25] P. Vaca, «Modelo de gestión de seguridad lógica de la información en la protección de los datos sensibles de los distritos de educación del Ecuador», Universidad Técnica de Ambato, p. 247, 2019.

[26] M. Perugachi, «Diseño de una política de seguridad de la información para la dirección de gestión económica de la ARCOTEL, basada en las normas ISO 27002:2013 y EGSI», Universidad Internacional SEK, p. 117, 2020.

[27] K. Peffers, T. Tuunanen, M. A. Rothenberger, y S. Chatterjee, «A design science research methodology for information systems research», J. Manag. Inf. Syst., vol. 24, n.o 3, pp. 45-77, 2007.

[28] Scandariato, R., Wuyts, K., & Joosen, W., «A descriptive study of Microsoft's threat modeling technique», de: «*Springer-Verlag*», p. 18, 2013.

[29] Shostack, A., «*Experiences Threat Modeling at Microsoft.*», Microsoft, p. 11, 2014.

[30] Kordy, P., & Schweitzer, P., «The *ADTool Manual*», Janvier, p. 27, 2015.

[31] We Live Security (2017, Jan 06). [Online]. Available: https://www.welivesecurity.com/la-es/videos/brechas-de-seguridad-en-2016/.

[32] We Live Security (2018, Jan 05). [Online]. Available: https://www.welivesecurity.com/la-es/2018/01/05/resumen-seguridad-2017-anio-llamados-atencion-parte-2/

[33] Bit Life media (2018, Jan 18). [Online]. Available: https://bitlifemedia.com/2018/12/las-mayores-brechas-de-datos-y-ciberataques-de-2018/

[34] We Live Security (2018, Dec 26). [Online]. Available: https://www.welivesecurity.com/la-es/2018/12/26/brechas-seguridad-exposicion-datos-mas-importantes-2018/

[35] Bit Life media (2020, Jan 02). [Online]. Available: https://bitlifemedia.com/2020/01/mayores-brechas-datos-seguridad-2019-actualizadas/

[36] D. Ram, K. Prakash y C. Joao, «Network risk management using attacker profiling», de: «SECURITY AND COMMUNICATION NETWORKS», p. 14, 2008.

[37] S. Kapetanakis, A. Filippoupolitis, G. Loukas, T. Murayziq, «Profiling cyber attackers using case-based reasoning.» de: "UK Workshop on Case-Based Reasoning (UKCBR 2014)", Cambridge, UK, 2014.

[38] J. Brynielsson, U. Franke, M. Adnan Tariq and S. Varga, «Using cyber defense exercises to obtain additional data for attacker profiling,», de: "2016 IEEE Conference on Intelligence and Security Informatics (ISI)", Tucson, AZ, 2016, pp. 37-42.

[39] A. Lenin, J. Willemson, D.P. Sari, «Attacker Profiling in Quantitative Security Assessment Based on Attack Trees.» de: "Lecture Notes in Computer Science", Springer, Cham, 2014.

[40] A. Lenin, «Performance analysis of attacker profiling in quantitative security risk assessment», Tallinn University of Technology, p. 46, 2014.

[41] B. Kordy, S. Mauw, S. Radomirović, P. Schweitzer, «Attribute Decoration of Attack–Defense Trees.» de: «Journal of Logic and Computation», p. 34, 2012.
[42] Shafiq, H., Asif, K., Shabir, A., Ghulam, R., & Sajid, I, «Threat modelling methodologies: a survey.», BahauddinZakariya University, 2014.
[43] Barzanallana R., «El método MAGERIT», Universidad de Murcia, p. 225, 2017.
[44] IT Sitio (2020, Jun 23). [Online]. Available: https://www.itsitio.com/pe/vulnerabilidades-los-dispositivos-iot/
[45] B Secure (2020, Sep 10). [Online]. https://www.b-secure.co/recursos/infografias/brechas-de-seguridad-en-iot
[46] Desarrollo NIC (2020, Jun 15). [Online]. https://desarrollonic.com/iot/#1526525128831-e004d062-1351

ANEXOS

Anexo I – Fichas Bibliográficas estado del arte

A.1 Ficha Bibliográfica 1

A.1.1 Referencia del texto

J. Pino, «Marco de Referencia para la implementación de un esquema gubernamental de seguridad de la información (EGSI), basado en la norma técnica ecuatoriana ISO/IEC 27001:2010 y en concordancia con el acuerdo 166», Quito: Universidad de la Américas, 2014.

A.1.2 Tema

Marco de Referencia para la implementación de un esquema gubernamental de seguridad de la información (EGSI), basado en la norma técnica ecuatoriana ISO/IEC 27001:2010 y en concordancia con el acuerdo 166.

A.1.3 Tesis

Es necesario que las instituciones públicas implementen EGSI, con sus debidas metodologías de gestión de riesgos.

A.1.4 Propósito

Elaborar un marco de referencia que incluya todas las actividades a ser ejecutadas para el diseño e implementación del Esquema Gubernamental de Seguridad de la Información en cualquier entidad pública del Ecuador.

A.1.5 Ideas centrales

El trabajo se divide en 3 partes.

Primero, un marco teórico, que abarca la información necesaria para entender la seguridad de la información, las normas internacionales ISO/IEC 27000 y los pasos para certificarse en la norma ISO/IEC 27001.

Segundo, el marco de referencia del EGSI, en este capítulo se hace un análisis de la normativa legal y técnica para este marco, su situación de cumplimiento en las instituciones publica y las actividades básicas para operar, mantener evaluar y mejorar el mismo.

Finalmente se presentan las conclusiones y recomendaciones respecto al marco elaborado.

A.1.6 Conceptos claves

Sistema de Gestión de Seguridad de la Información.

Acuerdo Ministerial 166 y el Esquema Gubernamental de Seguridad de la información.

Norma técnica ISO/IEC 27000.

Gestión de riesgos.

Riesgo residual.

Aplicabilidad de controles.

A.1.7 Conclusiones

La implementación del EGSI es el paso previo pata implementar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001.

El EGSI debe reforzar la evaluación de riesgos, pues está basado en ISO/IEC 27005, norma que provee lineamientos para la gestión de riesgos de seguridad de la información, pero no provee ninguna metodología específica para el análisis y la gestión de riesgos de la seguridad de la información.

EGSI provee una serie de controles administrativos, pero no los parámetros para la medición del cumplimiento de dichos controles.

EL EGSI tendrá éxito solo con el compromiso de toda la organización involucrada en su implementación.

A.2 Ficha Bibliográfica 2

A.2.1 Referencia del texto

C. Cáceres y C. Mena, «Elaboración de la guía de implantación de las normas prioritarias del esquema gubernamental de seguridad de la información EGSI en las entidades de la administración pública central». Escuela Politécnica Nacional, p. 209, 2015.

A.2.2 Tema

Elaboración de la guía de implantación de las normas prioritarias del esquema gubernamental de seguridad de la información EGSI en las entidades de la administración pública central.

A.2.3 Tesis

Colaborar en el proyecto de implantación del Esquema Gubernamental de la Información EGSI, determinando el estado inicial de la seguridad de la información, la definición de la política general de seguridad de la información y determinando los procedimientos para la implantación del EGSI.

A.2.4 Propósito

Elaborar una “Guía de implantación del Esquema Gubernamental de Seguridad de la Información EGSI”, definida para las entidades del sector público que pertenecen a la Administración Pública Central del Ecuador. También se valida la guía, tomando como caso de estudio la Agencia de Regulación y Control de la Electricidad.

A.2.5 Ideas centrales

El trabajo se divide en 4 capítulos.

Capítulo 1, análisis de la seguridad de la información en las entidades públicas del país, la normativa relacionada, análisis de EGSI frente al marco legal, métodos para el control y

seguimiento del proyecto y revisión de controles que tienen relación con Tecnologías de la información.

Capítulo 2, la guía para la implantación de EGSI, con lo pasos para definir la situación actual de seguridad de la información en la entidad, la política de seguridad de la información y los procedimientos para la aplicación de los controles de EGSI en las unidades de TU de la entidad.

Capítulo 3, validación de la guía, en la Agencia de Regulación y Control de Electricidad.

Capítulos 4, conclusiones y recomendaciones respecto a la elaboración de la guía.

A.2.6 Conceptos claves

Dominios claves de seguridad de la información: Confidencialidad, Disponibilidad e Integridad.

Normativa legal ecuatoriana frente a los dominios de seguridad de la información, Ley Orgánica de Transparencia de Acceso a la Información Pública (LOTAIP).

Marco Legal del Esquema Gubernamental de Seguridad de la Información (EGSI), Acuerdo Ministerial 166.

Análisis del contenido del EGSI.

Políticas de seguridad de la información.

A.2.7 Conclusiones

Para usar Guía de implantación de EGSI, es necesario que los involucrados conocer los estándares de TI sobre seguridad de la información, así como conocimientos de la normativa legal existente.

Es necesario validar la guía con un caso de estudio real, para ver su utilidad.

A.3 Ficha Bibliográfica 3

A.3.1 Referencia del texto

A. Pinto, «Análisis y planteamiento de políticas de acuerdo con el esquema gubernamental de seguridad de la información (EGSI) para la empresa pública Yachay». Universidad Técnica del Norte, p. 160, 2016.

A.3.2 Tema

Análisis y planteamiento de políticas de acuerdo con el esquema gubernamental de seguridad de la información (EGSI) para la empresa pública Yachay.

A.3.3 Tesis

El cumplimiento del EGSI exige a las empresas públicas que cumplan con Políticas de la Seguridad de la Información, lo que conlleva a las empresas a tomar la decisión a adquirir nuevas soluciones de seguridad u optimizar la existente. La puesta en producción de nuevos recursos tecnológicos implica un costo económico adicional a la planificación inicial.

Por el contrario, el planteamiento de políticas en base a una normativa internacional optimizaría las funcionalidades del equipamiento existente y revela los riesgos que no son cubiertos; lo que significaría una menor inversión.

A.3.4 Propósito

Plantear políticas en base al Esquema Gubernamental de Seguridad de la Información (EGSI) para la Empresa Pública Yachay con el fin de permitir ejecutar eficientemente los requisitos de seguridad

Analizar el Esquema Gubernamental de Seguridad de la Información (EGSI) dispuesto por la SNAP y los documentos que respaldan los procedimientos de Yachay E.P. para establecer los requerimientos de seguridad de información.

Describir el estado actual de la seguridad de información de Yachay E.P., normativa y prácticas de seguridad actuales.

Promover las mejores prácticas de seguridad al desarrollo de los sistemas de información, elaborando la propuesta de seguridad de información según los dominios, objetivos y controles.

Evaluar los procesos estableciendo un ambiente de pruebas, permitiendo obtener resultados para su posterior análisis y mejora continua.

A.3.5 Ideas centrales

El trabajo se divide en 4 partes.

Parte 1, describe los antecedentes, la problemática, los objetivos (general y específicos), el alcance y justificación que explican la ejecución del proyecto.

Parte 2, se detalla el fundamento teórico que es el soporte teórico de la investigación. Específicamente se mencionan los conceptos sobre la Normativa de Seguridad de la Información en base a la ISO/IEC 27002 y el Esquema Gubernamental de Seguridad; además se respalda la evaluación de riesgos en base a la herramienta MSAT y la propuesta de Políticas de Seguridad siguiendo la metodología de la Universidad Nacional de Colombia (Guía de Políticas de Seguridad de la Información), enmarcadas en los controles de la seguridad de la información. Así mismo, se hace un estudio de los procesos de seguridad de la información actuales en la Gerencia de Tecnologías de Yachay E.P y se plasma la documentación que respalda los mismos. Se realiza una evaluación de riesgos para identificar los activos críticos, establecer la magnitud de riesgos y plantear las medidas acordes a los requerimientos de la empresa. De esta manera, se identifica los controles de seguridad necesarios para la propuesta de las Políticas de Seguridad con fundamento en la Norma ISO/IEC 27002 y el EGSI.

Parte 3, se realiza la propuesta de Políticas de Seguridad de la Información con enfoque en la gestión de comunicaciones y operaciones, así como la documentación de desarrollo

de esta. Se presenta un bosquejo de políticas y se genera un escenario para el desarrollo que contiene la creación y revisión del proyecto.

Parte 4, se exponen los respectivos resultados obtenidos luego de los procesos de desarrollo, así como las recomendaciones de la presente investigación en la Empresa Pública Yachay

A.3.6 Conceptos claves

Seguridad de la Información.

Riesgo.

Evaluación y Gestión de Riesgo.

Metodologías para la evaluación de riesgos en las TI.

Política de seguridad.

Norma internacional ISO/IEC 27002.

Esquema Gubernamental de Seguridad (EGSI).

A.3.7 Conclusiones

La ejecución de proyectos enfocados a empresas públicas requiere de conocimientos de leyes, normas y reglamentos para estructurarlos de tal manera que se tenga un complemento entre el área técnica y las definiciones del Estado.

A.4 Ficha Bibliográfica 4

A.4.1 Referencia del texto

H. F. Gualotuña Guato y M. G. Quilumbaqui Muenala, «Aplicación de las normas técnicas ISO/IEC 27001 e ISO/IEC 27002 para el cumplimiento del esquema gubernamental de seguridad de la información (EGSI) en la infraestructura del sistema nacional de nivelación y admisión (SNNA)», Escuela Politécnica Nacional, p. 121, 2016.

A.4.2 Tema

Aplicación de las normas técnicas ISO/IEC 27001 e ISO/IEC 27002 para el cumplimiento del esquema gubernamental de seguridad de la información (EGSI) en la infraestructura del sistema nacional de nivelación y admisión (SNNA).

A.4.3 Tesis

Es necesario analizar, identificar y evaluar los riesgos, vulnerabilidades y amenazas a la que está expuesta la información para tomar sus debidos controles de seguridad para el manejo y transmisión de la información en la infraestructura del SNNA, basándose en las normas ISO/IEC 27001, 27002.

A.4.4 Propósito

Aplicar las normas técnicas ISO/IEC 27001 e ISO/IEC 27002 para cumplir con el esquema gubernamental de seguridad de la información (EGSI).

Analizar el acuerdo Ministerial 166.

Realizar un análisis, identificación, evaluación y tratamiento de los riesgos que presenta la Infraestructura del SNNA.

Elaborar políticas y Procedimientos de Seguridad de la Información para el SNNA.

A.4.5 Ideas centrales

El trabajo se divide en 3 partes.

Parte 1, se presentan generalidades y la identificación de la organización.

Parte 2, se realiza el análisis y gestión del riesgo para la SNNA, enmarcado en la norma ISO/IEC 27001:2013, usando MAGERIT.

Parte 3, se generan las conclusiones y recomendaciones del trabajo.

A.4.6 Conceptos claves

ISO/IEC 27001:2013.

Metodologías para la evaluación de riesgos en las TI.

MAGERIT.

Amenazas y vulnerabilidades.

Evaluación y Gestión de Riesgo.

Impacto residual.

Riesgo residual.

Política de seguridad.

Norma internacional ISO/IEC 27002.

Esquema Gubernamental de Seguridad (EGSI).

A.4.7 Conclusiones

Se escogió MAGERIT para el análisis y gestión del riesgo, ya que, está enfocada en la seguridad de la información.

La SNNA, tiene un nivel de cumplimiento de la norma ISO/IEC 27002 bajo, existen buenas prácticas, pero los procedimiento e incidentes de seguridad no han sido documentados.

A.5 Ficha Bibliográfica 5

A.5.1 Referencia del texto

C. Muyón, T. Guarda, G. Vargas, y G. Ninahualpa, «Esquema Gubernamental de Seguridad de la Información EGSI y su aplicación en las entidades públicas del Ecuador TT», Rev. Ibérica Sistemas. Y Tecnologías de la Información N.18, p. 9, 2018.

A.5.2 Tema

Esquema Gubernamental de Seguridad de la Información EGSI y su aplicación en las entidades públicas del Ecuador.

A.5.3 Tesis

Es necesaria una revisión del Esquema Gubernamental de Seguridad de la Información (EGSI) y su ámbito de acción.

A.5.4 Propósito

Presentar una conceptualización del Esquema Gubernamental de Seguridad de la información, dando a conocer su aplicabilidad, restricciones, practicas sugeridas, beneficios y sus posibles desventajas.

A.5.5 Ideas centrales

El trabajo se divide en 4 secciones.

La sección 1, presenta una descripción de la norma ISO/IEC 27001, su estructura, políticas, procedimientos, mecanismos de tratamiento de información y controles.

La sección 2, detalla la norma ISO/IEC 27002 y sus directrices de implementación.

La sección 3, realiza una descripción general del Esquema Gubernamental de Seguridad de la Información y su aplicación de manera específica en el Ministerio de Educación, se analiza los controles implementados en esa cartera de estado para verificar el nivel de cumplimiento de la norma EGSI.

La sección 4, exhibe las conclusiones.

A.5.6 Conceptos claves

ISO/IEC 27001.

ISO/IEC 27002.

Esquema Gubernamental de Seguridad (EGSI).

A.5.7 Conclusiones

El esquema gubernamental de seguridad de la información describe las actividades que se establecen para dar protección a los activos de información contra riesgos de pérdida, mal uso, divulgación o daño en las entidades públicas del Ecuador, su aplicación es obligatoria y es evaluada por la Contraloría General del Estado.

Es necesario que las instituciones sobre las cuales se rige esta normativa promuevan a los funcionarios los beneficios de buenas prácticas y comportamientos de seguridad de la información ofreciendo beneficios o recompensas por la buena cultura de seguridad aplicada.

Los funcionarios públicos a los cuales abarca la EGSI están aplicando solamente las prácticas más fundamentales de seguridad, sin embargo, se debe hacer mucho más.

A.6 Ficha Bibliográfica 6

A.6.1 Referencia del texto

A. Yánez, «Propuesta de controles de seguridad de la información desde el enfoque de protección de datos personales para los entes gubernamentales del Ecuador que tienen implementado la estrategia de gobierno en línea», Universidad Espíritu Santo, p. 35, 2018.

A.6.2 Tema

Propuesta de controles de seguridad de la información desde el enfoque de protección de datos personales para los entes gubernamentales del Ecuador que tienen implementado la estrategia de gobierno en línea.

A.6.3 Tesis

Las organizaciones deberán proponer políticas y controles apropiados que promuevan una gestión segura de los procesos del negocio, primando la protección de la información.

A.6.4 Propósito

Proponer los controles mínimos de seguridad de la información que, las instituciones públicas del Ecuador que tienen implementado el gobierno en línea y las organizaciones privadas (de todos los sectores), deberían poner en práctica para proteger los datos personales de los ciudadanos, que son administrados y procesados en su infraestructura tecnológica.

A.6.5 Ideas centrales

El trabajo se divide en 4 secciones.

La sección 1, presenta el marco teórico de la investigación, incluyendo seguridad de la información, datos personales, gobierno en línea, el Reglamento General de Protección de Datos (RGPD), ISO 27001.

La sección 2, detalla la metodología usada para proponer los controles de seguridad.

La sección 3, realiza análisis de la situación nacional e internacional, referente a la protección de datos personales.

La sección 4, exhibe las conclusiones.

A.6.6 Conceptos claves

ISO 27001.

ISO/IEC 27002.

Reglamento General de Protección de Datos RGPD.

Datos personales.

Gobierno en línea.

A.6.7 Conclusiones

En el Ecuador, las instituciones públicas que tienen implementado gobierno en línea no cuentan con una regulación que estipule los controles tecnológicos ni un marco referencial que facilite el establecimiento de medidas de seguridad de información para la protección de los datos personales.

La principal limitación para el presente trabajo de investigación es la ausencia de información sobre protección de datos personales en el Ecuador y de una ley específica sobre dicho tema.

Esta limitación también se convierte en una fortaleza porque permite ser pionero en la propuesta de controles para la protección de datos personales.

Dado el riesgo al cual están expuestos los datos personales se ha logrado implementar medidas de control en otros países incluido gran parte de países latinoamericanos, como Argentina, Uruguay, Colombia, Perú y México, y es muy probable que en el Ecuador deba ocurrir en un futuro cercano.

Los controles de protección de datos personales tienen estrecha relación con los controles de seguridad de la información lo que hace imprescindible que las instituciones públicas del Ecuador, que cuenten con gobierno en línea, deben tener implementado los controles de la norma técnica ecuatoriana NTE INEN-ISO/IEC 27001.

Se ha tomado como referencia esta norma, en virtud que el gobierno del Ecuador mediante la Secretaria Nacional de Administración Pública, con el fin de controlar el crecimiento de las TIC, asegurar la integridad, confidencialidad y disponibilidad de la información que reposa en las instituciones públicas; propuso la ejecución del Esquema Gubernamental de Seguridad de la Información (EGSI) que se basa en la norma NTE INEN ISO/IEC 27001:2011.

Por lo tanto, el presente trabajo servirá como punto de partida, para que las instituciones públicas ecuatorianas con gobierno en línea o aquellas que pretendan implementarlo, puedan administrar de manera óptima la seguridad de los datos personales de los ciudadanos al contar con una propuesta de controles basados en la Norma ISO/IEC 27001/2013.

De la misma manera este trabajo servirá como base para investigaciones futuras sobre la protección de datos personales en todas las instituciones públicas del Ecuador, además de las organizaciones privadas de todos los sectores.

Finalmente, el cuadro de controles propuesto debería ser considerado para su implementación en el sector privado.

A.7 Ficha Bibliográfica 7

A.7.1 Referencia del texto

M. Gallardo, «Elaboración de una política de seguridad de la información para una institución pública basado en el esquema gubernamental de seguridad de la información», Universidad Internacional SEK, p. 107, 2018.

A.7.2 Tema

Elaboración de una política de seguridad de la información para una institución pública basado en el esquema gubernamental de seguridad de la información.

A.7.3 Tesis

Las instituciones públicas deben cumplir los lineamientos relacionados a la aplicación del Esquema Gubernamental de Seguridad de la Información (EGSI), que fue emitido mediante Acuerdo Ministerial 166 en el año 2013 y se basa en las mejores prácticas de la norma ISO/IEC 270001-2.

A.7.4 Propósito

Plantear una Política de Seguridad de la Información, siguiendo las directrices del Esquema Gubernamental de Seguridad de la Información, lo que le permitirá garantizar la confidencialidad, disponibilidad e integridad de la información. Usando como caso de estudio el Ministerio de Telecomunicaciones.

A.7.5 Ideas centrales

El trabajo se divide en 4 capítulos.

El capítulo 1, presenta el planteamiento del problema y el marco teórico de la investigación.

El capítulo 2, realiza el análisis y diseño de las políticas de seguridad planteadas en base al EGSI, así como también plantea una metodología para la gestión de riesgos.

El capítulo 3, define la política de seguridad.

El capítulo 4, exhibe las conclusiones.

A.7.6 Conceptos claves

Sistema de Gestión de Seguridad de la Información (SGSI)

Esquema Gubernamental de Seguridad (EGSI).

Ciclo de Deming.

Gestión de Riesgos.

A.7.7 Conclusiones

La Institución pública (Ministerio de Telecomunicaciones), no tenía definida una metodología para tratamiento de riesgos y priorización de asignación de recursos, así como la mitigación mediante el uso de una política adecuada que permita brindar seguridad a las actividades de la institución.

Las aplicaciones críticas definidas en el estudio se alinearán a las definiciones establecidas en la política, considerando que los lineamientos propuestas aseguran la continuidad de estas y sobre soto resguardar la información ante cualquier tipo de amenaza interna o externa aplicada física o lógicamente.

La metodología aplicada se ajusta a la realidad de la Institución pública, por ende, a las instituciones públicas, considerando que varias no cuentan con una política de seguridad y de poseerla no se aplica, por lo cual con la metodología definida en esta investigación

prioriza y categoriza la criticidad de los aplicativos e infraestructura y mantener la continuidad del negocio, así como el tratamiento de los riesgos tecnológicos.

La política desarrollada cumple con los parámetros de confidencialidad, integridad y disponibilidad de la información aplicada a los activos críticos de la institución y se proyecta para una implementación y desarrollo de una política global orientada a los activos institucionales de acuerdo con la ponderación de su criticidad y riesgo para su tratamiento personalizado.

Con la ejecución de la política de seguridad de la información, la Institución pública, podrá cumplir a cabalidad con los hitos prioritarios definidos para la medición, conforme el acuerdo ministerial 166, patrocinado actualmente por el MINTEL.

A.8 Ficha Bibliográfica 8

A.8.1 Referencia del texto

C. López, «Gobierno De TI Basado En El Esquema Gubernamental De Seguridad De La Información (EGSI) En El Hospital San Luis De Otavalo», Universidad Técnica del Norte, p. 242, 2019.

A.8.2 Tema

Gobierno De TI Basado En El Esquema Gubernamental De Seguridad De La Información (EGSI) En El Hospital San Luis De Otavalo.

A.8.3 Tesis

Debido a las incidencias y brechas de seguridad del Hospital San Luis de Otavalo se ve la necesidad de implementar estándares que responden al cumplimiento de las disposiciones propuestas por la Secretaría Nacional de la Administración Pública, partiendo del análisis de la realidad de la estructura de TI, determinando los principales riesgos que no contribuyen a llevar a cabo un mejoramiento, garantía de calidad y transparencia en la prestación adecuada de Servicios de Salud.

A.8.4 Propósito

Diseñar un Gobierno de TI basado en el Esquema Gubernamental de la Seguridad de la Información (EGSI) en el Hospital San Luis de Otavalo.

Formular una Política de Seguridad de la Información a fin de mitigar o reducir los riesgos encontrados y que más se apeguen a los principios del EGSI.

A.8.5 Ideas centrales

El trabajo se divide en 5 capítulos.

El capítulo 1, presenta los antecedentes de la investigación.

El capítulo 2, consiste en un marco teórico y de referencia para el análisis de la seguridad de la información, incluyendo conceptos de COBIT 5, Análisis de riesgos según ISO/IEC

27005:2012, Esquema Gubernamental de Seguridad de la Información (EGSI), Norma ISO 27799:2008, normativa legal en el Ecuador.

El capítulo 3, diseña el gobierne de TI y realiza el análisis de riesgos del hospital San Luis de Otavalo.

El capítulo 4, formula e implementa las políticas de seguridad de la información.

El capítulo 5, presenta las conclusiones

A.8.6 Conceptos claves

COBIT 5.

Ley Orgánica de Transparencia de Acceso a la Información Pública (LOTAIP),

Esquema Gubernamental de Seguridad (EGSI).

ISO/EC 27005:2012.

Análisis de Riesgos.

A.8.7 Conclusiones

Con el marco de trabajo COBIT 5 se logró diseñar el Gobierno de TI para el Hospital San Luis de Otavalo a través de la aplicación de la técnica de la cascada de metas de COBIT 5 que consiste en alinear los objetivos estratégicos de la Institución con los objetivos, metas y procesos de TI propios de este marco de trabajo y que permitió determinar los procesos de TI que, en cuestiones de la Gestión de Riesgos y Seguridad de la Información, la Institución necesita mejorar; para ello, COBIT 5 como un marco integrador, se apoyó en otras normativas gubernamentales con un conjunto de buenas prácticas para mejorar aspectos específicos sobre la seguridad de la información.

La norma NTE INEN-ISO/IEC 27005:2015 permitió desarrollar el análisis de Gestión de Riesgos de la Seguridad de la Información de manera sistemática mediante lineamientos que explican cómo realizar la identificación de activos, el conocimiento de políticas existentes, la determinación de criterios para la valoración de activos y riesgos que, finalmente fueron expuestos en la matriz de riesgos, cuya información constituye el punto de partida para el tratamiento de las principales amenazas y vulnerabilidades asociadas con los activos de información críticos.

La solución para minimizar o reducir los riesgos presentes en la actual red de datos de la Institución fue por medio de la formulación la Política de Seguridad de la Información, un documento de alto nivel con medidas que exigen la importancia de proteger el activo más importante de esta casa de salud que es la información, y en especial, la información personal de los pacientes que a su vez es procesada por los equipos informáticos; se elaboró a partir de la inclusión del conjunto de buenas prácticas recomendadas por el Esquema Gubernamental de Seguridad de la Información (EGSI), así como de la normativa

NTE INEN-ISO 27799:2008 con aspectos específicos sobre la protección de la información en el ámbito sanitario.

La formulación de la Política de Seguridad de la Información se llevó a cabo mediante el establecimiento de procedimientos para tratar aspectos como la socialización de la Política de Seguridad de la Información, la formalización del acuerdo de Confidencialidad de la Información, el proceso a seguir para la gestión de riesgos e identificación de nuevas amenazas de riesgo y el procedimiento para la adquisición de licencias para uso de software propietario; adicionalmente, para mitigar los riesgos a nivel informático se utilizaron herramientas basadas principalmente en el uso de software libre para dar cumplimiento a políticas de seguridad específicas.

A.9 Ficha Bibliográfica 9

A.9.1 Referencia del texto

A. Zambrano, M. Jessica, P. Jocelin y L. Sebastiana, «La protección de datos personales: análisis de las leyes en el Ecuador», Escuela Superior Politécnica Agropecuaria de Manabí “Manuel Félix López”, p. 8, 2019.

A.9.2 Tema

La protección de datos personales: análisis de las leyes en el Ecuador.

A.9.3 Tesis

En Ecuador y demás países de América Latina, es necesario tener una normativa legal que proteja los datos personales de los ciudadanos.

A.9.4 Propósito

Realizar un estudio exploratorio de las leyes más relevantes que rigen la protección de datos en el Ecuador e identificar las sanciones a las que están expuestas las personas naturales y jurídicas en caso de adquirir información de manera ilegal, con la finalidad de que los ciudadanos conozcan en que reglamento se pueden amparar en el caso de que sus datos personales sean vulnerados.

A.9.5 Ideas centrales

El trabajo realiza un estudio de la normativa existente en Ecuador, pariendo de diversos casos de robo de información como el caso de Novaestrat del 2019, para discutir los resultados del estudio y emitir conclusiones.

A.9.6 Conceptos claves

Protección de datos.

Datos personales.

A.9.7 Conclusiones

Ecuador, al igual que Venezuela y Bolivia son en Latinoamérica los países que carecen de una ley de protección de datos personales, sin embargo, existen normativas que regulan de forma dispersa e imprecisa la protección de datos personales, puesto que no se especifica con claridad que es lo que se pretende proteger.

En el país se han presentados dos proyectos de ley para la protección de datos personales, el primer proyecto fue presentado en el 2016, mismo que no fue aprobado porque se incluían normas que limitaban el uso de las redes sociales lo que tergiversó la naturaleza de las propuestas. Un segundo proyecto fue presentado en septiembre de este año (2019), pero hasta la fecha no ha sido aprobado por la Asamblea Nacional.

De acuerdo con los resultados obtenidos se evidenció que el único reglamento que establece sanciones a las personas naturales y jurídicas que adquieren información de manera ilegal es el código Orgánico Integral Penal.

A.10 Ficha Bibliográfica 10

A.10.1 Referencia del texto

P. Vaca, «Modelo de gestión de seguridad lógica de la información en la protección de los datos sensibles de los distritos de educación del Ecuador», Universidad Técnica de Ambato, p. 247, 2019.

A.10.2 Tema

Modelo de gestión de seguridad lógica de la información en la protección de los datos sensibles de los distritos de educación del Ecuador.

A.10.3 Tesis

El modelo de gestión de la seguridad lógica de la información incide en la protección de los datos sensibles de los Distritos de Educación del Ecuador.

A.10.4 Propósito

Determinar cómo incide un modelo de gestión de seguridad lógica en la protección de la información sensible del Distrito de Educación 23D01 de la ciudad de Santo Domingo.

A.10.5 Ideas centrales

El trabajo consta de 6 capítulos.

El capítulo 1, contiene: el tema de investigación, el planteamiento del problema, su contexto, análisis crítico, prognosis, formulación del problema, interrogantes, delimitación, justificación y objetivos.

El capítulo 2, contiene: antecedentes de la investigación, fundamentación filosófica, fundamentación legal, categorías fundamentales, hipótesis y señalamiento de variables.

El capítulo 3, contiene: el enfoque de investigación, modalidad básica de la investigación, nivel o tipo de investigación, población y muestra, operacionalización de variables, plan de recolección de información y plan de procesamiento de la información.

El capítulo 4, contiene: análisis de resultados, formulario de evaluación y medición, validación de las respuestas obtenidas, interpretación del resultado del formulario de evaluación y medición.

El capítulo 5, contiene: las conclusiones y recomendaciones que se obtienen a partir de la investigación del marco teórico y el resultado de las respuestas que dan paso al desarrollo de la propuesta investigativa.

El capítulo 6, contiene: datos informativos, antecedentes de la propuesta, justificación, objetivos, análisis de factibilidad, elaboración de la propuesta, y el modelo de gestión de seguridad lógica de la información en la protección de los datos sensibles de los Distritos de Educación del Ecuador.

A.10.6 Conceptos claves

ISO 27000.

Datos personales.

Protección de Datos.

Ley Orgánica de Protección de Datos personales (LOPDP).

Marcos de trabajo en seguridad informática.

Metodologías de Análisis de Riesgos.

Ciclo de Deming.

Principio de “Defensa en Profundidad”.

Un Sistema de Gestión de Seguridad de la información (SGSI).

Habeas Data (HD).

Reglamento General de Protección de Datos (RGPD).

Proyecto de Ley de Orgánica de la Protección de los Derechos a la Intimidad y Privacidad.

Datos Sensibles.

Esquema Gubernamental de Seguridad de la Información (EGSI).

A.10.7 Conclusiones

Con la aplicación de las técnicas *pentesting* y de la encuesta se determina que la Dirección Distrital Educación 23D01 no cuenta con procesos estandarizados y que deban cumplirse para que los datos sensibles que en esta organización se genera, transmite y guarda sean protegidos ante cualquier vulnerabilidad.

Utilizando la metodología de análisis y gestión de riesgos de tecnologías de la información MAGERIT, permitió identificar el nivel de madurez en temas de seguridad de informática, con los que cuentan los funcionarios que aspectos como jefes departamentales de la

Dirección Distrital Educación 23D01, reflejando que la Dirección Distrital 23D01 no cuenta con un nivel aceptable en tema de protección de datos personales.

Al no tener un modelo de seguridad que sirva como lineamiento para la transmisión y protección de la información entre ella la de los datos sensibles y que llega a terceras personas que no sean tanto el concernido como los concernientes o encargados del tratamiento de esta puede generar que el Distrito de Educación se vea afectado en ámbitos legales, perdidas de reputación e imagen y también puede llegar a tener un desenlace con pérdidas económicas.

A.11 Ficha Bibliográfica 11

A.11.1 Referencia del texto

M. Perugachi, «Diseño de una política de seguridad de la información para la dirección de gestión económica de la ARCOTEL, basada en las normas ISO 27002:2013 y EGSI», Universidad Internacional SEK, p. 117, 2020.

A.11.2 Tema

Diseño de una política de seguridad de la información para la dirección de gestión económica de la ARCOTEL, basada en las normas ISO 27002:2013 y EGSI.

A.11.3 Tesis

La Dirección de Gestión Económica – DGE de la ARCOTEL, se encarga de recopilar, procesar y analizar la información financiera, entregada por los operadores de telecomunicaciones, misma que debe ser confiable, integra y disponible, pues es la base de los estudios sobre los cuales se determinan los informes de obligaciones de pago para el Estado, que son susceptibles de procesos de revisión por parte de la Contraloría General del Estado. Además, al ser una entidad pública, está obligada a cumplir con el Esquema de Gestión de Seguridad de la Información EGSI versión 2, emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información MINTEL, mediante acuerdo Nro. 25 de 10 de enero de 2020. El disponer de una política de seguridad de la información en la Dirección de Gestión Económica en ARCOTEL, ésta permitirá mitigar las vulnerabilidades y disminuir el impacto de los riesgos que presenta la gestión de la información, evitando la intrusión de agentes internos y externos a la organización, reduciendo futuros reclamos de operadores de telecomunicaciones y evitando egresos para el Estado.

A.11.4 Propósito

Diseñar una política de seguridad de la información para la Dirección de Gestión Económica de la ARCOTEL basada en las normas ISO 27002:2013 y en el EGSI, que permita la disponibilidad, integridad y confidencialidad de los datos**.**

Establecer los controles de seguridad mediante el análisis de la norma ISO 27002: 2013 que servirán para el diseño de la política de seguridad de la información de la Dirección de Gestión Económica de la ARCOTEL.

Establecer los controles de seguridad mediante el análisis de la norma ISO 27002: 2013 que servirán para el diseño de la política de seguridad de la información de la Dirección de Gestión Económica de la ARCOTEL.

A.11.5 Ideas centrales

EL trabajo consta de 5 capítulos.

El capítulo 1, planteamiento del problema de investigación, objetivos y justificaciones.

El capítulo 2, marco teórico, dimensiones de la seguridad de información, Gestión del Riesgo, norma ISO 27000, EGSI V2 y metodologías de gestión de riesgo.

El capítulo 3, análisis de situación actual y análisis de riesgos para el caso de estudio.

El capítulo 4, propuesta de la política de seguridad.

El capítulo 5, conclusiones y recomendaciones.

A.11.6 Conceptos claves

ISO 27000.

EGSI V2.

Metodologías de gestión de riesgo.

MAGERIT.

Gestión del Riesgo

A.11.7 Conclusiones

La identificación de los activos de información en la Dirección de Gestión Económica de la ARCOTEL se realizó utilizando la metodología de gestión de riesgos denominada MAGERIT, determinando nueve activos críticos, clasificados según la alta probabilidad de ocurrencia de las amenazas, así como al alto impacto que causaría en los activos de la Dirección.

Para reducir el riesgo de los activos de la información se identificó las vulnerabilidades que tenían los activos críticos de información y se escogió los controles de la norma ISO/IEC 27002 versión 2013, así como los sugeridos en el Esquema Gubernamental de Seguridad de la Información versión 2, emitido para las entidades del sector público del país que dependen del poder ejecutivo, como es el caso de la Dirección de Gestión Económica de la ARCOTEL.

La valoración de los activos de información, el análisis de las vulnerabilidades, categorización de amenazas y el impacto en la información de la Dirección de Gestión Económica, se realizó aplicando la metodología MAGERIT a través de las matrices de gestión de riesgos, con base a la experiencia de las actividades de valor agregado que

genera esta Dirección a la institución, así como a la estimación del riesgo sugerida por el EGSI versión 2 para las entidades del sector público.

La política se desarrolló para la Dirección de Gestión Económica de la ARCOTEL, seleccionando 22 controles en 9 áreas que proporciona la norma internacional ISO/IEC: 27002:2013, también se utilizó la guía para la implementación de los controles que ofrece el Esquema Gubernamental de Seguridad de la Información EGSI v2, tendientes a preservar y asegurar las dimensiones de la información.

La política de seguridad de la información propuesta permitirá reducir los riesgos de los activos de información a los que están sometidos la Dirección de Gestión Económica y en general el resto de las áreas de la ARCOTEL, contribuyendo a mejorar la gestión pública, la calidad de los informes, reduciendo futuros reclamos de operadores de telecomunicaciones, evitando egresos para el Estado y salvaguardando la confidencialidad, integridad y disponibilidad de la información.

Anexo II – Controles en base al formato de Declaración de Aplicabilidad, usando EGSI y RGPD

N°	CONTROL PROPUESTO	DESCRIPCIÓN	SECCIÓN ISO 27001:2013	SECCIÓN EGSI	SUSTRATO SECCIÓN RGPD	PREGUNTAS
C1	Establecer políticas para la gestión de datos personales sensibles	Establecer políticas revisadas y aprobadas por la Máxima autoridad de la Institución, que estipulen cuales son los datos personales sensibles que maneja la organización.	5.1.1 Políticas para la seguridad de la información	5.7.3 Aislar los servicios de procesamiento de información con datos sensibles y elementos que requieran protección especial, para reducir el riesgo de visualización de la información de personas no autorizadas.	4. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. Se respeta la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, expresión religiosa. 6. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar	¿La Institución posee prácticas, reglas, políticas o procedimientos definidos sobre el uso y la divulgación de datos personales que son de conocimiento de todos los actores del sistema de información? ¿La institución posee prácticas, reglas, políticas o procedimientos para el caso en que los usuarios del sistema de información pidieran justificación sobre todos los datos personales que existe sobre ellos? ¿La Institución posee políticas o procedimientos definidos para determinar qué datos son sensibles respecto a los usuarios de los sistemas de información?

N°	CONTROL PROPUESTO	DESCRIPCIÓN	SECCIÓN ISO 27001:2013	SECCIÓN EGSI	SUSTRATO SECCIÓN RGPD	PREGUNTAS
					aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.	
C2	Identificar y Asegurar activos fuera de la organización que contienen datos personales sensibles	Establecer mecanismos y controles, para registrar la salida fuera de las instalaciones de cualquier activo que contenga datos personales.	8.3.3 Transporte de medios físicos. 11.2.5 Retiro de activos. 11.2.6 Seguridad del equipo y activos fuera de las instalaciones.	5.11.1 Custodiar los equipos y medios que se encuentren fuera de las instalaciones de la institución. Tomar en cuenta las instrucciones del fabricante para la protección de los equipos que se encuentran fuera de estas instalaciones. 5.13.1 Tener autorización previa para el retiro de cualquier equipo,	15. La protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él.	¿La Institución posee prácticas, reglas, políticas o procedimientos definidos sobre el uso y la divulgación de datos personales que son de conocimiento de todos los actores del sistema de información? ¿La institución tiene normas claras sobre el manejo de activos externos que manejen datos sensibles?

N°	CONTROL PROPUESTO	DESCRIPCIÓN	SECCIÓN ISO 27001:2013	SECCIÓN EGSI	SUSTRATO SECCIÓN RGPD	PREGUNTAS
				información o software. 6.21.5 Adoptar controles especiales cuando sea necesario proteger información sensible, su divulgación y modificación.		
C3	Establecer estándares de configuración segura, desarrollo y actualización de los sistemas	Verificar que los sistemas que realizan el tratamiento de datos personales cuentan con configuraciones seguras.	14.1.3 Protección de las transacciones de servicios de aplicaciones. 14.2.1 Política de desarrollo seguro. 14.2.2 Procedimiento de control de cambios en sistemas.	8.1.2 (*) Definir los controles apropiados, tanto automatizados como manuales. 8.3.1 Incorporar controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores. 8.8.1 Definir y aplicar procesos de control de	49 Constituye un interés legítimo del responsable del tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los	¿Se protege la información mediante el uso de protocolos seguros, cifrado, firma electrónica, etc.? ¿Las aplicaciones de la institución cuentan con las configuraciones de seguridad adecuada para manejar datos sensibles?

N°	CONTROL PROPUESTO	DESCRIPCIÓN	SECCIÓN ISO 27001:2013	SECCIÓN EGSI	SUSTRATO SECCIÓN RGPD	PREGUNTAS
				cambios para la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.	datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes.	
C4	Establecer controles para la protección contra código malicioso.	Identificar y establecer los controles necesarios en la organización para evitar el código malicioso.	12.2.1 Controles contra el código malicioso. 12.6.2 Restricciones en la instalación de software.	6.10.1 (*) Prohibir el uso de software no autorizado por la institución. Elaborar un listado del software autorizado. 6.10.2 (*) Instalar y actualizar periódicamente software de antivirus y contra código malicioso.	49 Constituye un interés legítimo del responsable del tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios	¿Se tienen en cuenta los cambios, configuraciones, versiones, capacidad, rendimiento, problemas, incidentes, copias de seguridad, almacenamiento, restauración, registros de auditoría, alarmas / alertas, endurecimiento, evaluaciones de vulnerabilidad, parches, configuración / actualizaciones de antivirus, encriptación, etc.)? ¿La instalación software en los sistemas está limitada personal autorizado con privilegios de sistema adecuados?

N°	CONTROL PROPUESTO	DESCRIPCIÓN	SECCIÓN ISO 27001:2013	SECCIÓN EGSI	SUSTRATO SECCIÓN RGPD	PREGUNTAS
					conexos ofrecidos por, o accesibles a través de, estos sistemas y redes.	¿Los controles se aplican a parches, copias de seguridad y descargas de la web, así como a instalaciones de sistemas, servidores, etc.?
C5	Establecer reglas de control de acceso	Establecer reglas y privilegios para cada usuario o grupo de usuarios conforme a sus responsabilidades.	9.1.1 Política de control de acceso. 9.1.2 Acceso a las redes y a los servicios de red	6.13.2 Designar procedimientos y responsabilidades para la gestión de equipos remotos como el caso de redireccionamiento de puertos y accesos por Bps, incluyendo el área de operaciones y el área de usuarios finales. 6.14.3 Definir procedimientos para la utilización de los servicios de red para restringir el acceso a los servicios de red cuando sea necesario. 6.17.2 Establecer controles de	39. Todo tratamiento de datos personales debe ser lícito y leal. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento. 64. El responsable del tratamiento debe utilizar todas las medidas razonables para verificar la identidad de los interesados que soliciten acceso, en particular en el contexto de los servicios en línea y los identificadores en línea. El responsable no debe conservar datos	¿Existe una política de control de acceso? ¿Hay una segregación de deberes apropiada? ¿El proceso de aprobación requiere que se involucre el propietario del sistema o la información en cuestión? ¿Se asegura que el acceso VPN e inalámbrico es supervisado, controlados y autorizado? ¿Se utiliza autenticación de múltiples-factor para acceso a redes, sistemas y aplicaciones críticas, especialmente para los usuarios privilegiados?

N°	CONTROL PROPUESTO	DESCRIPCIÓN	SECCIÓN ISO 27001:2013	SECCIÓN EGSI	SUSTRATO SECCIÓN RGPD	PREGUNTAS
				acceso para evitar el acceso de personal no autorizado. 7.1.1 Gestionar los accesos de los usuarios a los sistemas de información, asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados.	personales con el único propósito de poder responder a posibles solicitudes. 83. El responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar	¿Cómo monitoriza la red para detectar acceso no autorizado? ¿Los controles de seguridad de la red son evaluados y probados regularmente (*Pentesting*)?

N°	CONTROL PROPUESTO	DESCRIPCIÓN	SECCIÓN ISO 27001:2013	SECCIÓN EGSI	SUSTRATO SECCIÓN RGPD	PREGUNTAS
					daños y perjuicios físicos, materiales o inmateriales.	
C6	Establecer políticas de cifrado de almacenamiento de datos.	Establecer políticas de cifrado para el almacenamiento de datos, así como de los controles y tipos de cifrado a implementar.	10.1.1 Políticas de uso de los controles criptográficos.	8.1.1 (*) Definir los requerimientos de seguridad. Por ejemplo: criptografía, control de sesiones, etc.	83. El responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.	¿La Institución cuenta con políticas de seguridad vigentes para cada grupo de datos personales? ¿La institución mantiene sus datos almacenados, correctamente cifrados dependiendo del nivel de sensibilidad de estos?

N°	CONTROL PROPUESTO	DESCRIPCIÓN	SECCIÓN ISO 27001:2013	SECCIÓN EGSI	SUSTRATO SECCIÓN RGPD	PREGUNTAS
C7	Gestionar privilegios de usuario	Conceder privilegios a cada usuario o grupo de usuarios, en ambiente multiusuario, en función de sus roles y responsabilidades para el cumplimiento de sus tareas.	9.2.2 Provisión de acceso de usuario. 9.2.3 Gestión de privilegios de acceso.	7.3.1 Controlar la asignación de privilegios a través de un proceso formal de autorización.	83. El responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.	¿El acceso a sistemas y servicios de información se basa en las necesidades del negocio? ¿Se garantiza que todo acceso que se concede se ajuste a las políticas de control de acceso y segregación de funciones? ¿Se controlan las actividades de los usuarios privilegiados de forma más detallada?
C8	Notificar vulneraciones de seguridad a titulares	Definir políticas y procedimientos notificación de vulneraciones a los	16.1.2 Notificación de los eventos de	9.1.1 (*) Instaurar un procedimiento formal para el reporte de los	85. Si no se toman a tiempo medidas adecuadas, las violaciones de la	¿Cómo se informan los eventos de seguridad de la información?

N°	CONTROL PROPUESTO	DESCRIPCIÓN	SECCIÓN ISO 27001:2013	SECCIÓN EGSI	SUSTRATO SECCIÓN RGPD	PREGUNTAS
		titulares cuando éstas afecten sus derechos patrimoniales o morales en lo referente a su información sensible.	seguridad de la información.	eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente, que establezca la acción que se ha de tomar al recibir el reporte sobre un evento que amenace la seguridad de la información	seguridad de los datos personales pueden entrañar daños y perjuicios. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.	¿Son conscientes los trabajadores de la necesidad de informar de inmediato y lo hacen? ¿Se crean informes de seguimiento de los incidentes? Desde la detección a la resolución.

N°	CONTROL PROPUESTO	DESCRIPCIÓN	SECCIÓN ISO 27001:2013	SECCIÓN EGSI	SUSTRATO SECCIÓN RGPD	PREGUNTAS
					87. Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado.	

Anexo III - Catálogo de Amenazas

ID	ID AMENAZA	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	CANAL	NIVEL	DESCRIPCIÓN
8	B1	Posible bloqueo o detención del proceso para el servidor web	Servidor Web	Denegación de servicio	HTTP	Alto	El navegador / Dispositivo móvil puede ser falsificado por un atacante y esto puede dar lugar a un acceso no autorizado al servidor web. Considere utilizar un mecanismo de autenticación estándar para identificar el proceso de origen.
9	B2	El flujo HTTP de datos puede potencialmente ser interrumpido	Servidor Web	Denegación de servicio	HTTP	Alto	Servidor web puede ser falsificado por un atacante y esto puede dar lugar a la divulgación de información por parte del navegador / dispositivo móvil. Considere utilizar un mecanismo de autenticación estándar para identificar el proceso de destino.
22	B3	Consumo potencial excesivo de recursos para Aplicación web / Sitio web o Base de Datos	Servidor Web	Denegación de servicio	Conexión	Alto	Los datos que fluyen a través de HTTP pueden ser manipulados por un atacante. Esto puede llevar a un ataque de denegación de servicio contra Servidor web o un ataque de elevación de privilegios contra Servidor web o una divulgación de información por parte de Servidor web. No verificar que la entrada sea la esperada es la causa principal de una gran cantidad de problemas explotables. Considere todas las rutas y la forma en que manejan los datos. Verifique que se verifique que todas las entradas sean correctas utilizando un enfoque de validación de entradas de lista aprobada.

ID	ID AMENAZA	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	CANAL	NIVEL	DESCRIPCIÓN
27	B4	Consumo potencial excesivo de recursos para Gestor de base de datos o Base de Datos	Servidor Web	Denegación de servicio	Conexión	Alto	El servidor web 'Servidor web' podría estar sujeto a un ataque de scripts entre sitios porque no desinfecta la entrada que no es de confianza.
29	B5	Potencial Consumo Excesivo de Recursos para Servidor web externo o Base de datos en la nube	Servidor web externo	Denegación de servicio	llamada	Alto	Servidor web afirma que no recibió datos de una fuente fuera del límite de confianza. Considere utilizar el registro o la auditoría para registrar la fuente, la hora y el resumen de los datos recibidos.
37	B6	La conexión del flujo de datos se interrumpe potencialmente	Aplicación Web	Denegación de servicio	Conexión	Alto	Un atacante puede detectar los datos que fluyen a través de HTTP. Dependiendo del tipo de datos que pueda leer un atacante, puede usarse para atacar otras partes del sistema o simplemente ser una divulgación de información que conduce a violaciones de cumplimiento. Considere cifrar el flujo de datos.
38	B7	Almacén de datos inaccesible	Servidor Web	Denegación de servicio	Conexión	Alto	El servidor web se bloquea, se detiene, se detiene o se ejecuta lentamente; en todos los casos violando una métrica de disponibilidad.
44	B8	La conexión del flujo de datos se interrumpe potencialmente	Servidor Web	Denegación de servicio	Conexión	Alto	Un agente externo interrumpe el flujo de datos a través de un límite de confianza en cualquier dirección.
45	B9	Almacén de datos inaccesible	Servidor Web	Denegación de servicio	Conexión	Alto	Servidor web puede hacerse pasar por el contexto del navegador / dispositivo móvil para obtener privilegios adicionales.

ID	ID AMENAZA	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	CANAL	NIVEL	DESCRIPCIÓN
51	B10	Posible bloqueo o detención del proceso para el navegador / dispositivo móvil	Servidor Web	Denegación de servicio	Uso	Alto	El navegador / Dispositivo móvil puede ejecutar código de forma remota para el servidor web.
52	B11	La interfaz IOCTL de flujo de datos está potencialmente interrumpida	Servidor Web	Denegación de servicio	Uso	Alto	Un atacante puede pasar datos al Servidor web para cambiar el flujo de ejecución del programa dentro del Servidor web a elección del atacante.
10	B12	Elevación mediante suplantación	Navegador / Dispositivo Móvil	Elevación de privilegios	HTTP	Alto	Usuario Externo puede ser engañado por un atacante y esto puede dar lugar a un acceso no autorizado al Navegador / Dispositivo móvil. Considere utilizar un mecanismo de autenticación estándar para identificar la entidad externa.
11	B13	El servidor web puede estar sujeto a la elevación de privilegios mediante la ejecución remota de código	Servidor Web	Elevación de privilegios	HTTP	Alto	El navegador / Dispositivo móvil puede hacerse pasar por el contexto de Usuario Externo para obtener privilegios adicionales.
12	B14	Elevación cambiando el flujo de ejecución en Servidor web	Servidor Web	Elevación de privilegios	HTTP	Alto	Aplicación web / Sitio web puede hacerse pasar por el contexto de Servidor web para obtener privilegios adicionales.
14	B15	Elevación mediante suplantación	Base de Datos	Elevación de privilegios	Uso	Alto	Base de Datos puede ser falsificada por un atacante y esto puede llevar a que los datos se escriban en el objetivo del atacante en lugar de Base de Datos. Considere utilizar un mecanismo de autenticación estándar para identificar el almacén de datos de destino.

ID	ID AMENAZA	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	CANAL	NIVEL	DESCRIPCIÓN
19	B16	Elevación mediante suplantación	Aplicación Web	Elevación de privilegios	Llamada	Alto	La inyección SQL es un ataque en el que se inserta código malicioso en cadenas que luego se pasan a una instancia de SQL Server para su análisis y ejecución. Cualquier procedimiento que construya declaraciones SQL debe revisarse para detectar vulnerabilidades de inyección porque SQL Server ejecutará todas las consultas sintácticamente válidas que reciba. Incluso los datos parametrizados pueden ser manipulados por un atacante hábil y decidido.
24	B17	Elevación mediante suplantación	Aplicación Web	Elevación de privilegios	Uso	Alto	¿Aplicación web / Sitio web o Base de Datos toman medidas explícitas para controlar el consumo de recursos? Los ataques de consumo de recursos pueden ser difíciles de manejar, y hay ocasiones en las que tiene sentido dejar que el sistema operativo haga el trabajo. Tenga cuidado de que sus solicitudes de recursos no se bloqueen y de que se agoten el tiempo de espera.
31	B18	Elevación mediante suplantación	Base de Datos	Elevación de privilegios	HTTP	Alto	Usuario Interno puede ser engañado por un atacante y esto puede dar lugar a un acceso no autorizado al Gestor de base de datos. Considere utilizar un mecanismo de autenticación estándar para identificar la entidad externa.
53	B19	Elevación mediante suplantación	Base de Datos	Elevación de privilegios	Uso	Alto	Gestor de base de datos puede hacerse pasar por el contexto de Usuario Interno para obtener privilegios adicionales.

ID	ID AMENAZA	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	CANAL	NIVEL	DESCRIPCIÓN
54	B20	El navegador / dispositivo móvil puede estar sujeto a la elevación de privilegios mediante la ejecución remota de código	Base de Datos	Elevación de privilegios	Uso	Alto	Base de Datos puede ser falsificada por un atacante y esto puede llevar a que los datos se escriban en el objetivo del atacante en lugar de Base de Datos. Considere utilizar un mecanismo de autenticación estándar para identificar el almacén de datos de destino.
55	B21	Elevación al cambiar el flujo de ejecución en el navegador / dispositivo móvil	Aplicación Web	Elevación de privilegios	Uso	Alto	La inyección SQL es un ataque en el que se inserta código malicioso en cadenas que luego se pasan a una instancia de SQL Server para su análisis y ejecución. Cualquier procedimiento que construya declaraciones SQL debe revisarse para detectar vulnerabilidades de inyección porque SQL Server ejecutará todas las consultas sintácticamente válidas que reciba. Incluso los datos parametrizados pueden ser manipulados por un atacante hábil y decidido.
7	B22	Detección de flujo de datos	Base de Datos	Divulgación de información	HTTP	Alto	¿Gestor de base de datos o Base de Datos toma medidas explícitas para controlar el consumo de recursos? Los ataques de consumo de recursos pueden ser difíciles de manejar, y hay ocasiones en las que tiene sentido dejar que el sistema operativo haga el trabajo. Tenga cuidado de que sus solicitudes de recursos no se bloqueen y de que se agoten el tiempo de espera.
35	B23	Detección de flujo de datos	Base de datos en la Nube	Divulgación de información	Conexión	Alto	La Base de datos en la nube puede ser falsificada por un atacante y esto puede llevar a que los datos se escriban en el objetivo del atacante en lugar de la Base de datos en la nube. Considere utilizar un mecanismo de autenticación estándar para identificar el almacén de datos de destino.

ID	ID AMENAZA	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	CANAL	NIVEL	DESCRIPCIÓN
36	B24	Tránsito de credenciales débil	Servidor Web Externo	Divulgación de información	Conexión	Alto	¿El Servidor web externo o la Base de datos en la nube toman medidas explícitas para controlar el consumo de recursos? Los ataques de consumo de recursos pueden ser difíciles de manejar, y hay ocasiones en las que tiene sentido dejar que el sistema operativo haga el trabajo. Tenga cuidado de que sus solicitudes de recursos no se bloqueen y de que se agoten el tiempo de espera.
42	B25	Detección de flujo de datos	Servidor Web Externo	Divulgación de información	Conexión	Alto	El servidor web 'Servidor web externo' podría estar sujeto a un ataque de scripting entre sitios porque no desinfecta la entrada que no es de confianza.
43	B26	Tránsito de credenciales débil	Servidor Web Externo	Divulgación de información	Conexión	Alto	Servidor web externo puede hacerse pasar por el contexto de Navegador / Dispositivo móvil para obtener privilegios adicionales.
50	B27	Detección de flujo de datos	Aplicación Web	Divulgación de información	Uso	Alto	Aplicación web / Sitio web puede ser falsificado por un atacante y esto puede dar lugar a un acceso no autorizado a Base de Datos. Considere utilizar un mecanismo de autenticación estándar para identificar el proceso de origen.
6	B28	Rechazo potencial de datos por parte del servidor web	Base de Datos	Repudio	HTTP	Alto	Los datos que fluyen a través de Conexión pueden ser manipulados por un atacante. Esto puede conducir a la corrupción de la Base de Datos. Asegure la integridad del flujo de datos al almacén de datos.

ID	ID AMENAZA	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	CANAL	NIVEL	DESCRIPCIÓN
34	B29	Data Store niega que la base de datos pueda escribir datos	Base de Datos	Repudio	Conexión	Alto	Base de Datos afirma que no escribió datos recibidos de una entidad en el otro lado del límite de confianza. Considere utilizar el registro o la auditoría para registrar la fuente, la hora y el resumen de los datos recibidos.
41	B30	Data Store niega que la base de datos pueda escribir datos	Base de Datos	Repudio	Conexión	Alto	Un atacante puede rastrear los datos que fluyen a través de Conexión. Dependiendo del tipo de datos que pueda leer un atacante, puede usarse para atacar otras partes del sistema o simplemente ser una divulgación de información que conduce a violaciones de cumplimiento. Considere cifrar el flujo de datos.
49	B31	Posible rechazo de datos por parte del navegador / dispositivo móvil	Aplicación Web	Repudio	Uso	Alto	Las credenciales en un mensaje a menudo están sujetas a ser detectadas por un atacante. ¿Las credenciales son reutilizables / reproducibles? ¿Se incluyen las credenciales en un mensaje? Por ejemplo, enviando un archivo zip con la contraseña en el correo electrónico. Utilice criptografía sólida para la transmisión de credenciales. Utilice las bibliotecas del sistema operativo si es posible y considere la agilidad del algoritmo criptográfico, en lugar de codificar una opción.
2	B32	Suplantar el proceso del navegador / dispositivo móvil	Aplicación Web	Suplantación	HTTP	Alto	Un agente externo interrumpe el flujo de datos a través de un límite de confianza en cualquier dirección.
3	B33	Suplantación del proceso web del servidor	Servidor Web	Suplantación	HTTP	Alto	Un agente externo evita el acceso a un almacén de datos en el otro lado del límite de confianza.

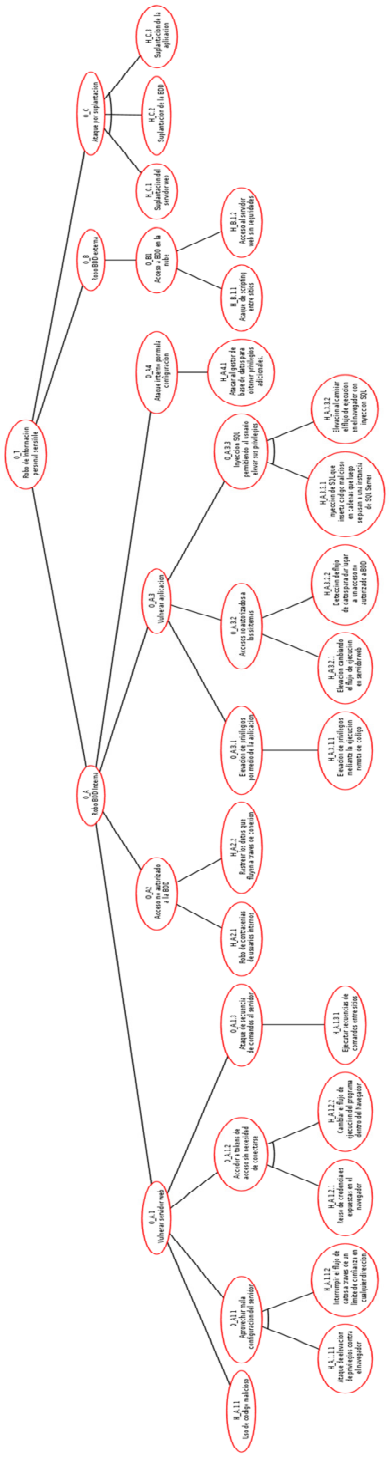
ID	ID AMENAZA	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	CANAL	NIVEL	DESCRIPCIÓN
13	B34	Suplantación de la entidad externa Usuario Externo	Base de Datos	Suplantación	Uso	Alto	Gestor de base de datos puede ser falsificado por un atacante y esto puede dar lugar a un acceso no autorizado a Base de Datos. Considere utilizar un mecanismo de autenticación estándar para identificar el proceso de origen.
20	B35	Suplantación de la base de datos del almacén de datos de destino	Base de Datos	Suplantación	Conexión	Alto	Los datos que fluyen a través de Conexión pueden ser manipulados por un atacante. Esto puede conducir a la corrupción de la Base de Datos. Asegure la integridad del flujo de datos al almacén de datos.
23	B36	Suplantación de la entidad externa Usuario Interno	Base de Datos	Suplantación	Uso	Alto	Base de Datos afirma que no escribió datos recibidos de una entidad en el otro lado del límite de confianza. Considere utilizar el registro o la auditoría para registrar la fuente, la hora y el resumen de los datos recibidos.
25	B37	Suplantación de la base de datos del almacén de datos de destino	Base de Datos	Suplantación	Conexión	Alto	Un atacante puede rastrear los datos que fluyen a través de Conexión. Dependiendo del tipo de datos que pueda leer un atacante, puede usarse para atacar otras partes del sistema o simplemente ser una divulgación de información que conduce a violaciones de cumplimiento. Considere cifrar el flujo de datos.

ID	ID AMENAZA	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	CANAL	NIVEL	DESCRIPCIÓN
28	B38	Suplantación del almacenamiento destino de Base de datos en la nube	Base de Datos en la nube	Suplantación	llamada	Alto	Las credenciales en el mensaje a menudo están sujetas a ser detectadas por un atacante. ¿Las credenciales son reutilizables / reproducibles? ¿Se incluyen las credenciales en un mensaje? Por ejemplo, enviando un archivo zip con la contraseña en el correo electrónico. Utilice criptografía sólida para la transmisión de credenciales. Utilice las bibliotecas del sistema operativo si es posible y considere la agilidad del algoritmo criptográfico, en lugar de codificar una opción.
32	B39	Suplantación del proceso Aplicación web / Sitio web	Aplicación Web	Suplantación	Conexión	Alto	Un agente externo interrumpe el flujo de datos a través de un límite de confianza en cualquier dirección.
39	B40	Suplantación del proceso Gestor de base de datos	Base de Datos	Suplantación	Conexión	Alto	Un agente externo evita el acceso a un almacén de datos en el otro lado del límite de confianza.
46	B41	Suplantar el proceso del navegador / dispositivo móvil	Navegador / Dispositivo Móvil	Suplantación	Uso	Alto	El navegador / Dispositivo móvil puede ser engañado por un atacante y esto puede dar lugar a la divulgación de información por parte del Usuario Interno. Considere utilizar un mecanismo de autenticación estándar para identificar el proceso de destino.
47	B42	Suplantación de la entidad externa Usuario Interno	Navegador / Dispositivo Móvil	Suplantación	Uso	Alto	Usuario Interno puede ser engañado por un atacante y esto puede dar lugar a un acceso no autorizado al Navegador / Dispositivo móvil. Considere utilizar un mecanismo de autenticación estándar para identificar la entidad externa.

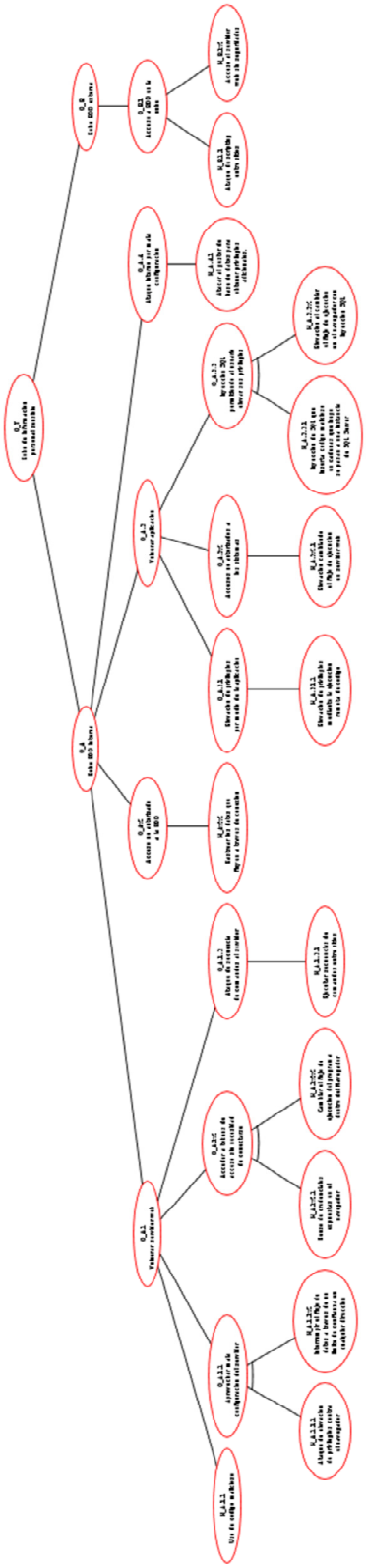
ID	ID AMENAZA	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	CANAL	NIVEL	DESCRIPCIÓN
4	B43	Posible falta de validación de entrada para el servidor web	Servidor Web	Manipulación	HTTP	Alto	Los datos que fluyen a través de Uso pueden ser manipulados por un atacante. Esto puede dar lugar a un ataque de denegación de servicio contra el navegador / dispositivo móvil o un ataque de elevación de privilegios contra el navegador / dispositivo móvil o una divulgación de información por parte del navegador / dispositivo móvil. No verificar que la entrada sea la esperada es la causa principal de una gran cantidad de problemas explotables. Considere todas las rutas y la forma en que manejan los datos. Verifique que se verifique que todas las entradas sean correctas utilizando un enfoque de validación de entradas de lista aprobada.
5	B44	Secuencias de comandos entre sitios	Aplicación Web	Manipulación	HTTP	Alto	Browser / Dispositivo móvil afirma que no recibió datos de una fuente fuera del límite de confianza. Considere utilizar el registro o la auditoría para registrar la fuente, la hora y el resumen de los datos recibidos.
21	B45	Potencial vulnerabilidad de inyección de SQL para la base de datos	Aplicación Web	Manipulación	Conexión	Alto	Los datos que fluyen a través de Uso pueden ser olfateados por un atacante. Dependiendo del tipo de datos que pueda leer un atacante, puede usarse para atacar otras partes del sistema o simplemente ser una divulgación de información que conduce a violaciones de cumplimiento. Considere cifrar el flujo de datos.
26	B46	Potencial vulnerabilidad de inyección de SQL para la base de datos	Navegador / Dispositivo Móvil	Manipulación	Conexión	Alto	El navegador / Dispositivo móvil se bloquea, se detiene, se detiene o se ejecuta lentamente; en todos los casos violando una métrica de disponibilidad.

ID	ID AMENAZA	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	CANAL	NIVEL	DESCRIPCIÓN
30	B47	Secuencias de comandos entre sitios	Aplicación Web	Manipulación	HTTP	Alto	Un agente externo interrumpe el flujo de datos a través de un límite de confianza en cualquier dirección.
33	B48	El almacén de datos de la Base de Datos podría estar dañado	Aplicación Web	Manipulación	Conexión	Alto	El navegador / Dispositivo móvil puede hacerse pasar por el contexto de Usuario Interno para obtener privilegios adicionales.
40	B49	El almacén de datos de la Base de Datos podría estar dañado	Base de Datos	Manipulación	Conexión	Alto	Usuario Interno puede ejecutar código de forma remota para el navegador / dispositivo móvil.
48	B50	Posible falta de validación de entrada para el navegador / dispositivo móvil	Aplicación Web	Manipulación	Uso	Alto	Un atacante puede pasar datos al Navegador / Dispositivo móvil para cambiar el flujo de ejecución del programa dentro del Navegador / Dispositivo móvil a elección del atacante.

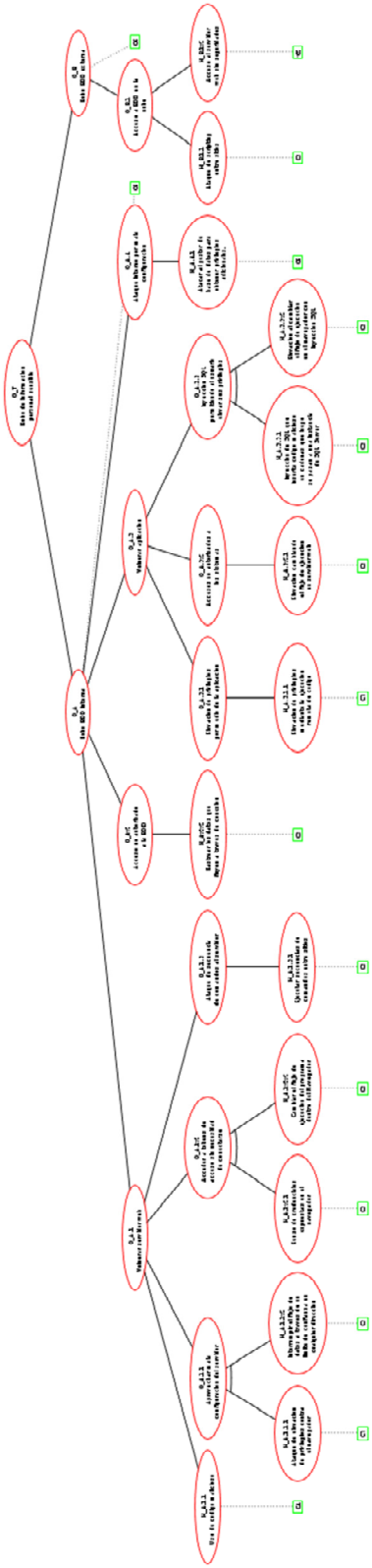
Anexo IV - Árbol global "Robo de Información Sensible"



Anexo V - Árbol de ataque final "Robo de Información Sensible"



Anexo VI - Árbol de defensa "Robo de Información Sensible"



Anexo VII - Evaluación de un ambiente "Internet de las Cosas"

1 DEFINICIÓN DEL ESCENARIO IOT

1.1 IDENTIFICACIÓN DEL ESCENARIO IOT

Usando el método propuesto en [15], se utilizaron los siguientes valores:

Tema: Brechas de seguridad que afectan "*Internet of Things*" IOT.

El límite espacio temporal: informes del año 2020.

Palabras claves: Brecha, seguridad, IOT.

Subtemas: brechas de seguridad, IOT.

Al realizar una búsqueda de términos exactos y términos relacionados en títulos y capítulos en los motores de búsqueda se encontró un aproximado de 99.900 páginas que cumplían las características indicadas, por este motivo, se procedió a depurar la búsqueda y seleccionar los reportes que resumen las brechas y las vulnerabilidades que afectan a IOT, de esta manera se utilizan las referencias [44] [45].

Se presenta un resumen de las principales brechas detectadas en base a la búsqueda realizada y considerando el Modelo STRIDE que usa *Microsoft Threat Modelling Tool*.

Tabla 25 - Resumen brechas de seguridad IOT

DISPOSITIVO	INFORMACIÓN COMPROMETIDA	MÉTODO USADO O DEBILIDAD APROVECHADA	CATEGORÍA STRIDE	TIPO DE ATACANTE
Monitores de bebé	Audios de niños y sus alrededores.	Puertos abiertos exponían el dispositivo a cualquier persona en Internet y revelaban información confidencial del usuario.	Divulgación de información, Elevación de privilegios, Manipulación, Suplantación	Externo
Vehículos	Tomaron control del vehículo a distancia.	El servidor de automatización expuesto contenía información importante como la geolocalización del domicilio y las contraseñas codificadas.	Divulgación de información, Elevación de privilegios	Externo
Impresoras	Documentos que se imprimían.	La interfaz no requería de contraseña.	Manipulación	Externo
Televisores	Imágenes y audios de los usuarios.	Puertos abiertos exponían el dispositivo a cualquier persona en Internet y revelaban información confidencial del usuario.	Divulgación de información, Elevación de privilegios,	Externo

DISPOSITIVO	INFORMACIÓN COMPROMETIDA	MÉTODO USADO O DEBILIDAD APROVECHADA	CATEGORÍA STRIDE	TIPO DE ATACANTE
			Manipulación, Suplantación	
Equipo Médico	Datos personales y registros médicos	Puertos abiertos exponían el dispositivo a cualquier persona en Internet y revelaban información confidencial del usuario.	Divulgación de información, Elevación de privilegios, Manipulación, Suplantación	Externo
Cámaras de seguridad	Grabaciones de seguridad.	Se usaban las contraseñas por defecto de las cámaras	Divulgación de información, Manipulación, Suplantación	Externo

Se puede apreciar en la Tabla 26, que el objetivo primordial de los atacantes es “El robo de información sensible”, con esta información se procede a elaborar un primer un catálogo de amenazas.

Tabla 26 - Catálogo de amenazas inicial IOT

ID	ACTIVOS COMPROMETIDOS	MÉTODO USADO O DEBILIDAD APROVECHADA	CATEGORÍA STRIDE	TIPO DE ATACANTE
A1	Puertas de acceso IOT	Puertos abiertos exponían el dispositivo a cualquier persona en Internet y revelaban información confidencial del usuario.	Divulgación de información, Elevación de privilegios, Manipulación, Suplantación	Externo
A2	Dispositivo IOT	El servidor de automatización expuesto contenía información importante como la geolocalización del domicilio y las contraseñas codificadas.	Divulgación de información, Elevación de privilegios	Externo
A3	Dispositivo IOT	La interfaz no requería de contraseña o usaba contraseña por defecto.	Divulgación de información, Manipulación, Suplantación	Externo
A4	Dispositivo IOT	El dispositivo permitía ejecutar código externo.	Manipulación	Externo

1.2 MODELO DE SISTEMA IOT

En base a la Tabla 26, y con referencia a [46] se propone una infraestructura experimental que permite analizar las potenciales amenazas que afectaron redes IOT que reportaron brechas de seguridad y que por motivos confidencialidad no fueron revelados de manera clara y total.

- Dispositivos IOT, con claves por defecto o sin claves.
- Redes locales, con puertos abiertos o mal configurados.
- Aplicaciones de terceros, que pueden dar servicios a los dispositivos IOT.
- Servidores de terceros que almacenan las aplicaciones.
- *Browser* o dispositivos móviles, son los medios de acceso desde el exterior a los dispositivos.

Utilizando *Microsoft Threat Modeling Tool*, se modela la infraestructura experimental, este modelado permite enriquecer el escenario propuesto de manera que permita analizar las posibles amenazas que afectaron a las organizaciones.

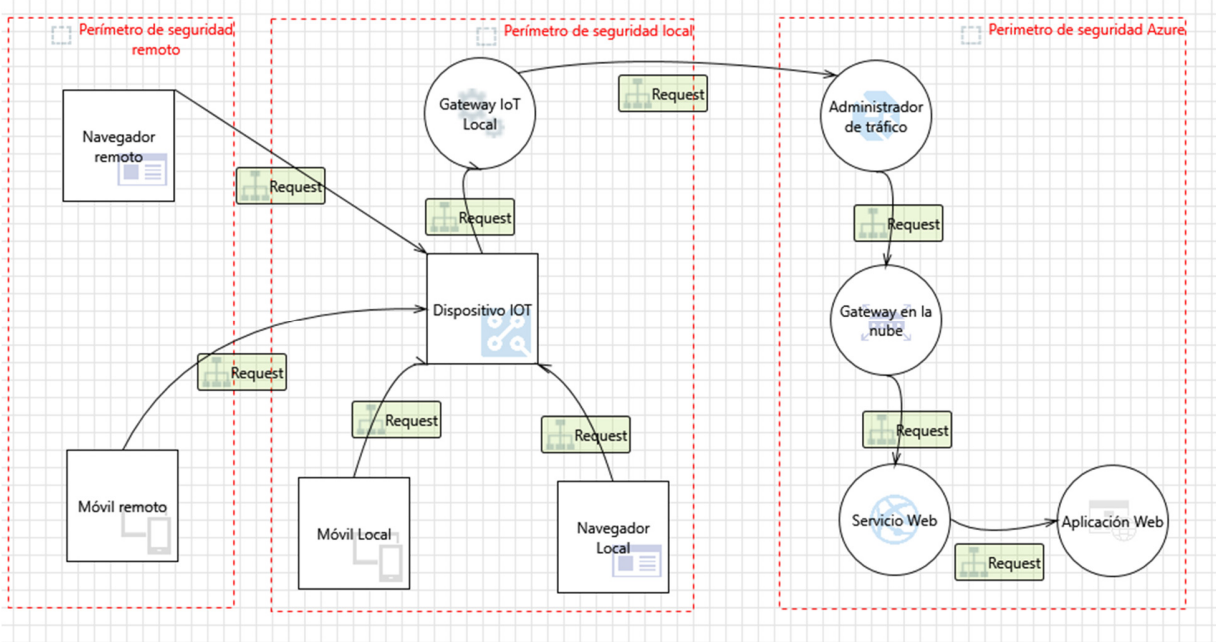


Figura 34 - Infraestructura IOT

1.3 MODELO DE ATAQUE IOT

Considerando la Tabla 26 y la Figura 34, se puede describir el siguiente modelo de ataque:

Un usuario externo mediante un dispositivo móvil o un navegador puede ganar acceso a los distintos dispositivos IOT mediante el uso de credenciales que los dispositivos tienen por defecto o por la ausencia de claves.

Un usuario externo mediante un dispositivo móvil o un navegador puede acceder a los dispositivos IOT aprovechando puertos expuestos.

2 CICLO DE GESTIÓN DE RIESGOS IOT

Tomando en cuenta el escenario tipo de estudio, se realizará un ciclo de gestión de riesgos, recorriendo cada una de las etapas propuestas

2.1 ESTABLECER CONTEXTO

En la sección anterior se pudo especificar el escenario tipo con los modelos de ataque y sistema, mismos que constituyen el contexto a analizar, el siguiente paso en el establecimiento del contexto consiste en estratificar tanto los perfiles del atacante como el catálogo de amenazas.

2.1.1 Perfil de atacantes IOT

Considerando los lineamientos de [36], [37] y [38] y en base a la información recolectada de los casos de brechas de seguridad IOT reportados, se hace tiene que los atacantes son:

Atacantes externos, aquellas personas que sin ser los propietarios de los dispositivos IOT acceden a ellos con fin de realizar actividades mal intencionadas aprovechando el mal manejo de claves o puertos físicos de los dispositivos.

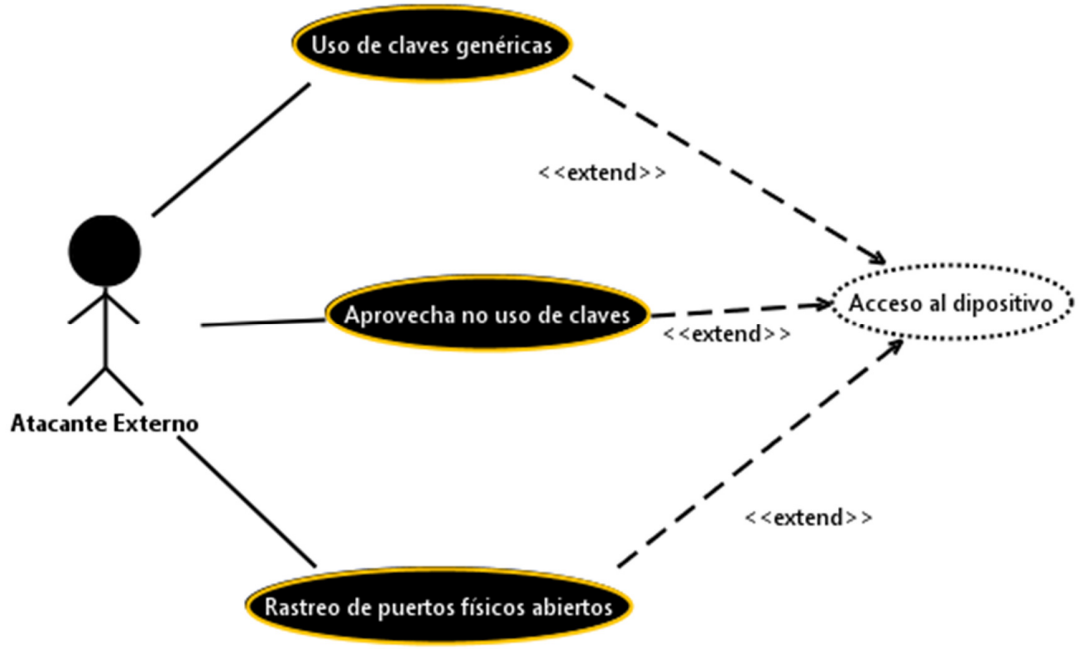


Figura 35 - Diagrama de casos de mal uso de atacantes externos IOT

Usando los lineamientos de la Tabla 6, se puede especificar a los atacantes con una habilidad media, un presupuesto bajo y tiempo de días para realizar sus actividades, pues con esto es suficiente para conseguir sus objetivos

Tabla 27 - Perfiles de atacantes IOT

ATACANTES	**HABILIDAD**	**PRESUPUESTO USD**	**TIEMPO**
Externos	M	B	D

2.1.2 Catálogo de amenazas IOT

Con el uso *Microsoft Thread Modeling Tool* 2016, utilizando como punto de partida la infraestructura propuesta y el esquema de ataque, en base a la revisión de brechas de seguridad IOT se obtiene el catálogo de amenazas, que se puede ver en detalle en el Anexo E.

Al trabajar con amenazas que afectan la privacidad se eliminaran del catálogo conseguido todas las amenazas que no influyen en este aspecto, también al estar modelando el ataque desde la perspectiva de las personas que poseen los dispositivos IOT, se eliminaran las amenazas que afectan a las empresas que ofrecen los servicios que estos dispositivos usan.

Con estos lineamientos y considerando el catálogo de amenazas inicial, se obtiene el siguiente catálogo de amenazas enriquecido

Tabla 28 - Catálogo de amenazas IOT

ID	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	NIVEL	DESCRIPCIÓN	ID CATÁLOGO BRECHAS	DESCRIPCIÓN TIPO
B1	Un adversario puede escuchar a escondidas la comunicación entre el dispositivo y la puerta de enlace de campo.	Gateway IOT	Divulgación de información	Alto	Un adversario puede escuchar a escondidas e interferir con la comunicación entre el dispositivo y la puerta de enlace de campo y posiblemente alterar los datos que se transmiten.	A1	Puertos abiertos exponían el dispositivo a cualquier persona en Internet y revelaban información confidencial del usuario.
B2	Un adversario puede obtener acceso a datos confidenciales de archivos de registro	Gateway IOT	Divulgación de información	Alto	Un adversario puede obtener acceso a datos confidenciales de archivos de registro	A1	Puertos abiertos exponían el dispositivo a cualquier persona en Internet y revelaban información confidencial del usuario.
B3	Un adversario puede obtener acceso a datos confidenciales rastreando el tráfico del cliente móvil	Gateway IOT	Divulgación de información	Alto	Un adversario puede obtener acceso a datos confidenciales rastreando el tráfico del cliente móvil	A1	Puertos abiertos exponían el dispositivo a cualquier persona en Internet y revelaban información confidencial del usuario.
B4	Un adversario puede revertir contenido con cifrado débil o hash	Dispositivo IOT	Divulgación de información	Alto	Un adversario puede revertir contenido con cifrado débil o hash	A3	La interfaz no requería de contraseña o usaba contraseña por defecto.
B5	Un adversario puede explotar servicios o funciones no utilizados en Gateway IoT Local	Gateway IOT	Elevación de privilegios	Alto	Un adversario puede usar funciones o servicios no utilizados en Gateway IoT Local, como interfaz de usuario, puerto USB, etc. Las funciones no utilizadas aumentan la superficie de ataque y	A1	Puertos abiertos exponían el dispositivo a cualquier persona en Internet y revelaban información confidencial del usuario.

ID	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	NIVEL	DESCRIPCIÓN	ID CATÁLOGO BRECHAS	DESCRIPCIÓN TIPO
					sirven como puntos de entrada adicionales para el adversario		
B6	Un adversario puede obtener acceso no autorizado a funciones privilegiadas en Dispositivo IOT	Dispositivo IOT	Elevación de privilegios	Alto	Un adversario puede obtener acceso a la interfaz de administración o servicios privilegiados como Wifi, SSH, archivos compartidos, FTP, etc., en un dispositivo	A2	El servidor de automatización expuesto contenía información importante como la geolocalización del domicilio y las contraseñas codificadas.
B7	Un adversario puede obtener acceso no autorizado a funciones privilegiadas en Gateway IoT Local	Gateway IOT	Elevación de privilegios	Alto	Un adversario puede obtener acceso a la interfaz de administración o servicios privilegiados como Wifi, SSH, archivos compartidos, FTP, etc., en un dispositivo	A1	Puertos abiertos exponían el dispositivo a cualquier persona en Internet y revelaban información confidencial del usuario.
B8	Un adversario puede ejecutar código desconocido en Dispositivo IOT	Dispositivo IOT	Manipulación	Alto	Un adversario puede lanzar código malicioso en Dispositivo IOT y ejecutarlo	A4	El dispositivo permitía ejecutar código externo.
B9	Un adversario puede ejecutar código desconocido en Gateway IoT Local	Gateway IOT	Manipulación	Alto	Un adversario puede lanzar código malicioso en Gateway IoT Local y ejecutarlo		

ID	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	NIVEL	DESCRIPCIÓN	ID CATÁLOGO BRECHAS	DESCRIPCIÓN TIPO
B10	Un adversario puede explotar vulnerabilidades conocidas en dispositivos no parcheados	Dispositivo IOT	Manipulación	Alto	Un adversario puede aprovechar las vulnerabilidades conocidas y explotar un dispositivo si el firmware del dispositivo no está actualizado.		
B11	Un adversario puede manipular el Dispositivo IOT y extraer material de clave criptográfica de él.	Dispositivo IOT	Manipulación	Alto	Un adversario puede reemplazar parcial o totalmente el software que se ejecuta en Gateway IoT Local, lo que podría permitir que el software reemplazado aproveche la identidad genuina del dispositivo si el material clave o las instalaciones criptográficas que contienen materiales clave estuvieran disponibles para el programa ilícito.	A3	La interfaz no requería de contraseña o usaba contraseña por defecto.

ID	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	NIVEL	DESCRIPCIÓN	ID CATÁLOGO BRECHAS	DESCRIPCIÓN TIPO
B12	Un adversario puede manipular Gateway IoT Local y extraer material de clave criptográfica de él.	Gateway IOT	Manipulación	Alto	Un adversario puede reemplazar parcial o totalmente el software que se ejecuta en el Administrador de tráfico, permitiendo potencialmente que el software reemplazado aproveche la identidad genuina del dispositivo si el material clave o las instalaciones criptográficas que contienen materiales clave estuvieran disponibles para el programa ilícito.		
B13	Un adversario puede obtener acceso no autorizado a IoT Field Gateway y alterar su sistema operativo	Gateway IOT	Manipulación	Alto	Un adversario puede obtener acceso no autorizado a Gateway IoT Local, manipular su sistema operativo y obtener acceso a información confidencial en el Gateway de campo.	A1	Puertos abiertos exponían el dispositivo a cualquier persona en Internet y revelaban información confidencial del usuario.

ID	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	NIVEL	DESCRIPCIÓN	ID CATÁLOGO BRECHAS	DESCRIPCIÓN TIPO
B14	Un adversario puede falsificar un dispositivo y conectarse a la puerta de enlace de campo	Gateway IOT	Suplantación	Alto	Un adversario puede falsificar un dispositivo y conectarse a la puerta de enlace de campo. Esto se puede lograr incluso cuando el dispositivo está registrado en la puerta de enlace de la nube, ya que la puerta de enlace de campo puede no estar sincronizada con las identidades del dispositivo en la puerta de enlace de la nube.	A1	Puertos abiertos exponían el dispositivo a cualquier persona en Internet y revelaban información confidencial del usuario.
B15	Un adversario puede obtener acceso a la puerta de enlace de campo aprovechando las credenciales de inicio de sesión predeterminadas.	Gateway IOT	Suplantación	Alto	Un adversario puede obtener acceso a la puerta de enlace de campo aprovechando las credenciales de inicio de sesión predeterminadas.	A1	Puertos abiertos exponían el dispositivo a cualquier persona en Internet y revelaban información confidencial del usuario.
B16	Un adversario puede reutilizar los tokens de autenticación de Dispositivo IOT en otro	Dispositivo IOT	Suplantación	Alto	Un atacante puede extraer material de clave criptográfica de Dispositivo IOT, ya sea a nivel de software o hardware, y posteriormente acceder al sistema con un Dispositivo IOT físico o virtual diferente bajo la identidad del Dispositivo IOT del que se ha	A3	La interfaz no requería de contraseña o usaba contraseña por defecto.

ID	AMENAZA / VULNERABILIDAD	ACTIVO	TIPO	NIVEL	DESCRIPCIÓN	ID CATÁLOGO BRECHAS	DESCRIPCIÓN TIPO
					extraído el material de clave		

2.2 EVALUACIÓN DE RIESGOS

Para evaluar los riesgos del escenario tipo, se utilizarán tanto el catálogo de amenazas, como los perfiles de atacantes, para crear arboles de ataque que permitan cuantificar el riesgo inherente

2.2.1 Generación de árboles de ataque IOT

En base al catálogo de amenazas generado con el uso de la herramienta ADTool, se genera el siguiente árbol de ataque para el escenario tipo a usarse, este árbol va a ser divido por sus objetivos principales para mejor comprensión [30]:

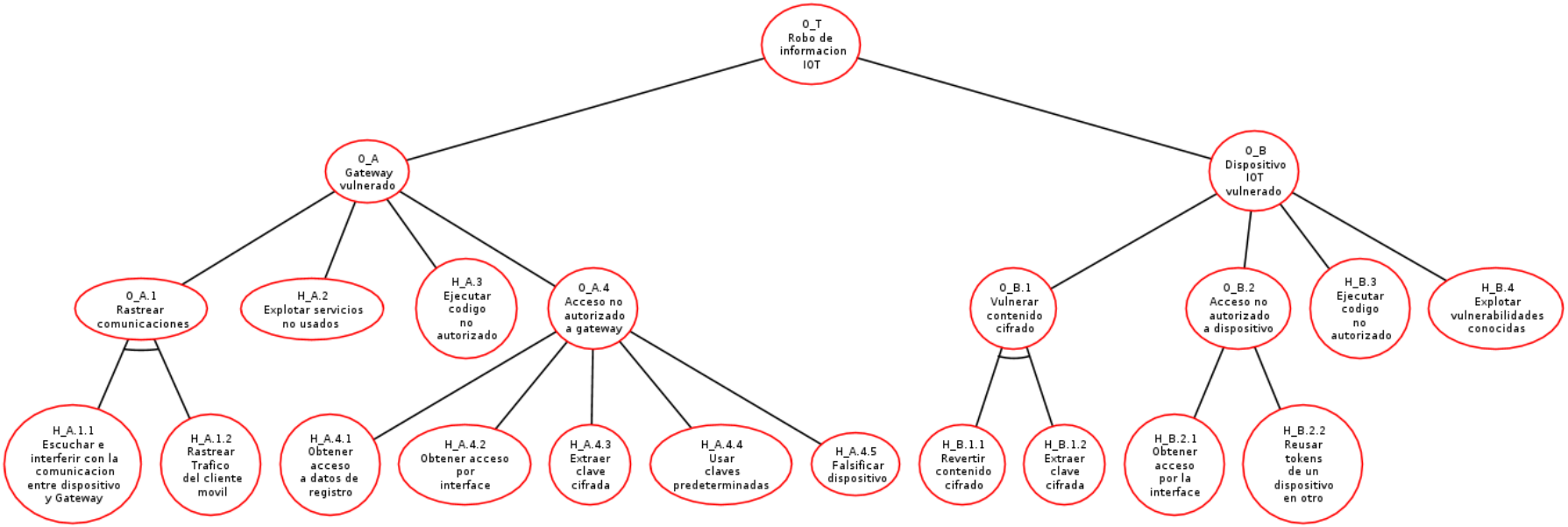


Figura 36 - Árbol de ataque "Robo de Información IOT"

2.2.2 Definición de atributos y valores para nodos hijos IOT

Como primer paso se procede a detallar los nodos del árbol generado. Con el objetivo de entender el mismo de manera más sencilla.

Tabla 29. Codificación del árbol de ataque “Robo de información IOT”

CÓDIGO	DESCRIPCIÓN	CÓDIGO DE AMENAZA
H_A.1.1	Escuchar e interferir con la comunicación entre dispositivo y Gateway	B1
H_A.1.2	Rastrear tráfico del cliente móvil.	B3
H_A.2	Explotar servicios no usados	B5
H_A.3	Ejecutar código no autorizado	B9
H_A.4.1	Obtener acceso a datos de registro	B2
H_A.4.2	Obtener acceso por interfaz	B7
H_A.4.3	Extraer clave cifrada	B12
H_A.4.4	Usar claves predeterminadas	B15
H_A.4.5	Falsificar dispositivo	B14
H_B.1.1	Revertir contenido cifrado	B4
H_B.1.2	Extraer clave cifrada	B11
H_B.2.1	Obtener acceso por la interfaz	B6
H_B.2.2	Reusar tokens de un dispositivo en otro	B16
H_B.3	Ejecutar código no autorizado	B8
H_B.4	Explotar vulnerabilidades conocidas	B10
O_A.1	Rastrear comunicaciones	
O_A.4	Acceso no autorizado a Gateway	B13
O_B.1	Vulnerar contenido cifrado	
O_B.2	Acceso no autorizado a dispositivo	
O_A	Gateway vulnerado	
O_B	Dispositivo IOT vulnerado	
O_T	Robo de información IOT	

Los atributos usados en cada uno de los nodos del árbol de ataque serán todos los indicados por la Tabla 10, y los valores asignados están propuestos en base a la búsqueda sistemática de escenarios de brechas.

Tabla 30 - Valores de atributos iniciales del árbol de ataque “Robo de información IOT”

Nodo	Atacante	Costo	Impacto	Habilidad	Probabilidad	Riesgo
H_A.1.1	Externo	1.0000	7.0000	0.5000	0.7000	2.4500
H_A.1.2	Externo	1.0000	7.0000	0.5000	0.6500	2.2750
H_A.2	Externo	1.0000	8.0000	0.5000	0.7000	2.8000
H_A.3	Externo	1.0000	9.0000	0.5000	0.6500	2.9250
H_A.4.1	Externo	1.0000	8.0000	0.5000	0.7000	2.8000
H_A.4.2	Externo	1.0000	8.0000	0.5000	0.9000	3.6000
H_A.4.3	Externo	1.0000	8.0000	0.5000	0.5000	2.0000
H_A.4.4	Externo	1.0000	8.0000	0.5000	0.9000	3.6000
H_A.4.5	Externo	2.0000	9.0000	0.5000	0.6000	1.3500
H_B.1.1	Externo	1.0000	7.0000	0.5000	0.6000	2.1000
H_B.1.2	Externo	1.0000	8.0000	0.5000	0.6000	2.4000
H_B.2.1	Externo	1.0000	7.0000	0.5000	0.9000	3.1500
H_B.2.2	Externo	1.0000	8.0000	0.5000	0.8000	3.2000
H_B.3	Externo	1.0000	9.0000	0.5000	0.6500	2.9250
H_B.4	Externo	1.0000	9.0000	0.5000	0.7000	3.1500

2.2.3 Propagación de valores IOT

Con el árbol de ataque definido y previo al cálculo del riesgo inherente es necesario propagar los atributos por todos los nodos. Para conseguir este objetivo, se utilizará la codificación de la Tabla 11 y las fórmulas de la Tabla 13.

Tabla 31 - Propagación de atributos por el árbol de ataque “Robo de información IOT”

CÓDIGO	COSTO	IMPACTO	HABILIDAD	PROBABILIDAD	RIESGO
H_A.1.1	1.0000	7.0000	0.5000	0.7000	2.4500
H_A.1.2	1.0000	7.0000	0.5000	0.6500	2.2750
H_A.2	1.0000	8.0000	0.5000	0.7000	2.8000
H_A.3	1.0000	9.0000	0.5000	0.6500	2.9250
H_A.4.1	1.0000	8.0000	0.5000	0.7000	2.8000
H_A.4.2	1.0000	8.0000	0.5000	0.9000	3.6000
H_A.4.3	1.0000	8.0000	0.5000	0.5000	2.0000

CÓDIGO	COSTO	IMPACTO	HABILIDAD	PROBABILIDAD	RIESGO
H_A.4.4	1.0000	8.0000	0.5000	0.9000	3.6000
H_A.4.5	2.0000	9.0000	0.5000	0.6000	1.3500
H_B.1.1	1.0000	7.0000	0.5000	0.6000	2.1000
H_B.1.2	1.0000	8.0000	0.5000	0.6000	2.4000
H_B.2.1	1.0000	7.0000	0.5000	0.9000	3.1500
H_B.2.2	1.0000	8.0000	0.5000	0.8000	3.2000
H_B.3	1.0000	9.0000	0.5000	0.6500	2.9250
H_B.4	1.0000	9.0000	0.5000	0.7000	3.1500
O_A.1	2.0000	9.1000	0.5000	0.4550	1.0351
O_A.4	1.1667	9.0000	0.5000	0.9994	3.8547
O_B.1	2.0000	9.4000	0.5000	0.3600	0.8460
O_B.2	1.0000	8.0000	0.5000	0.9800	3.9200
O_A	1.2216	9.1000	0.5000	1.0000	3.7246
O_B	1.1338	9.4000	0.5000	0.9987	4.1400
O_T	1.1778	9.4000	0.5000	1.0000	3.9905

Para entender de manera más clara como se obtienen los valores de los atributos por todo el árbol, se utilizarán los nodos O_A.1.1 y O_B.1 Para ejemplificar los cálculos en nodos *AND* y *OR* se utilizarán los nodos O_A.1 y O_B.2 respectivamente.

Para calcular los valores del nodo O_A.1 se deben usar los valores de los nodos O_A.1.1 y O_A.1.2 con una relación *AND*.

Costo O_A.1 = Costo O_A.1.1 + Costo O_A.1.2

Costo O_A.1 = 1 + 1

Costo O_A.1 = 2

Impacto O_A.1 $= \frac{10^2-\left((10-Impacto\ O\_A.1.1)x(10-Impacto\ O\_A.1.2)\right)}{10^{(2-1)}}$

Impacto O_A.1 $= \frac{100-((10-7)x(10-7))}{10^{(1)}}$

Impacto O_A.1 $= \frac{100-(9)}{10^{(1)}}$

Impacto O_A.1 = 9.1

Habilidad O_A.1 $= Max_{1=1}^{2}(Habilidad\ O\_A.1.1 : Habilidad\ O\_A.1.2)$

Habilidad O_A.1 $= Max\ (0.50 : 0.50)$

Habilidad O_A.1 $= 0.50$

Probabilidad O_A.1 = Probabilidad O_A.1.1 x Probabilidad O_A.1.2

Probabilidad O_A.1 = 0.70 * 0.65

Probabilidad O_A.1 = 0.455

Riesgo O_A.1 = $\frac{(\text{Probabilidad O\_A.1 x Impacto O\_A.1 x Habilidad O\_A.1})}{Costo\ O\_A.1}$

Riesgo O_A.1 = $\frac{(0.455 \text{ x } 9.1 \text{ x } 0.5)}{2}$

Riesgo O_A.1 = 1.0351

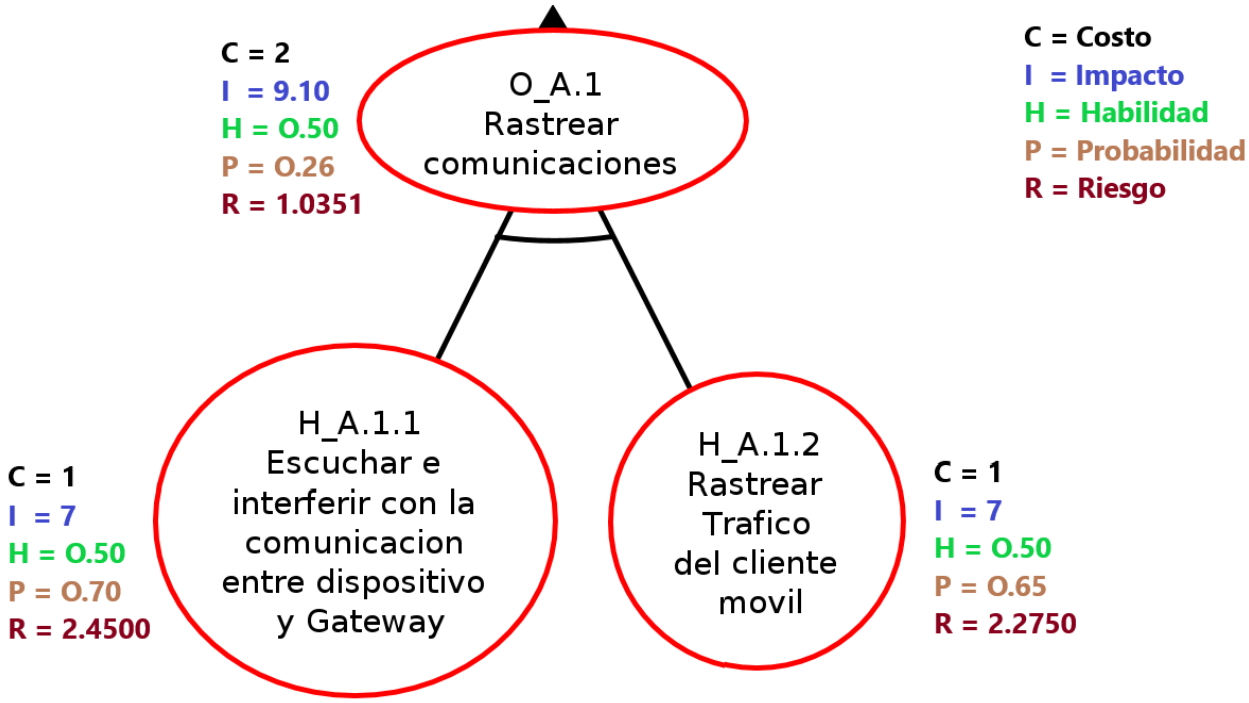


Figura 37 - Cálculo de atributos en nodo AND

Para calcular los valores del nodo O_B.2 se deben usar los valores de los nodos O_B.2.1 y O_B.2.2 con una relación OR.

Usando las fórmulas de la Tabla 13, se tiene:

Costo O_B.2 = $\frac{((Probabilidad\ O\_B.2.1\ x\ Costo\ O\_B.2.1\ )+(Probabilidad\ O_B.2.2\ x\ Costo\ O\_B.2.2))}{(Probabilidad\ O\_B.2.1 + Probabilidad\ O\_B.2.2)}$

Costo O_B.2 = $\frac{((0.90\ x\ 1)+(0.80\ x\ 1))}{(0.90+ 0.80)}$

Costo O_B.2 = $\frac{((0.90)+(0.80))}{(1.70)}$

Costo O_B.2 = 1

Impacto O_B.2 = $Max\ (Impacto\ O\_B.2.1 : Impacto\ O\_B.2.2)$

Impacto O_B.2 $= Max\ (7 : 8)$

Impacto O_B.2 = 8

Habilidad O_B.2 $= Min\ (Habilidad\ O\_B.2.1 : Habilidad\ O\_B.2.2)$

Habilidad O_B.2 $= Min\ (0.5 : 0.5)$

Habilidad O_B.2 $= 0.5$

Probabilidad O_B.2 = 1-(1-Probabilidad O_B.2.1) x (1-Probabilidad O_B.2.2)

Probabilidad O_B.2 = 1-((1-0.90) x (1-0.80))

Probabilidad O_B.2 = 1-((0.10) x (0.20))

Probabilidad O_B.2 = 1-(0.02)

Probabilidad O_B.2 = 0.98

Riesgo O_B.2 $= \frac{(\text{Probabilidad O\_B.2 x Impacto O\_B.2 x Habilidad O\_B.2})}{Costo\ O\_B.2}$

Riesgo O_B.2 $= \frac{(0.98 \text{ x } 8 \text{ x } 0.5)}{1}$

Riesgo O_B.2 = 3.9200

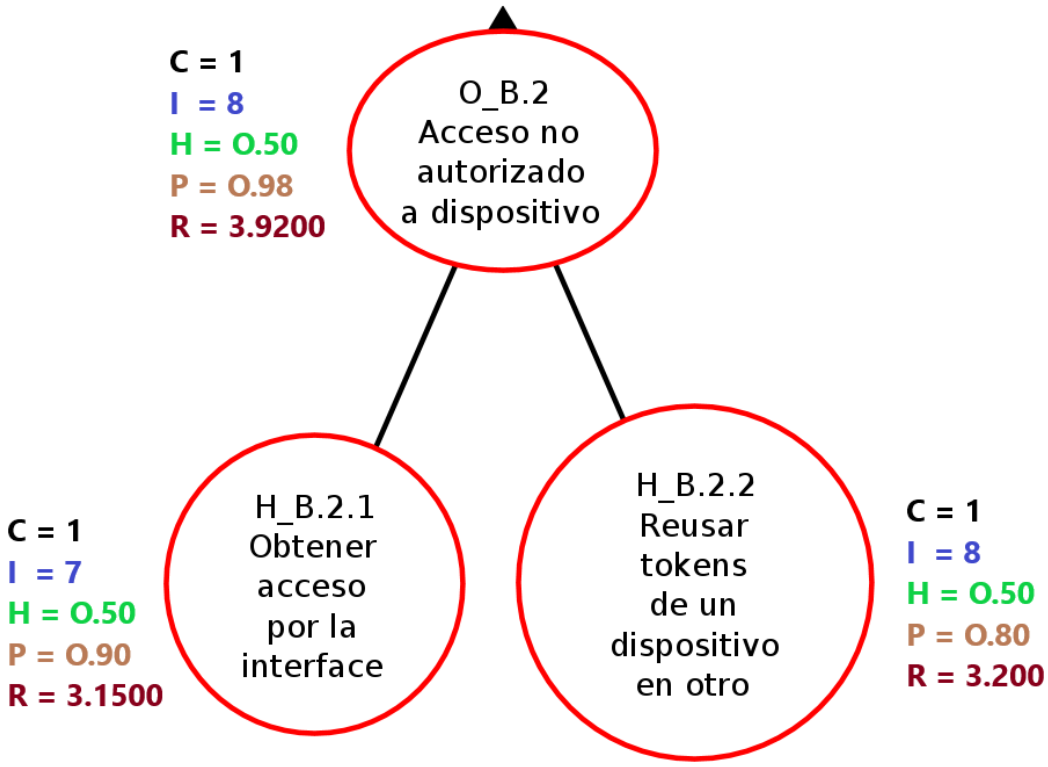


Figura 38 - Cálculo de atributos en nodo OR

2.2.3 Cálculo y valoración del riesgo inherente IOT

Al trabajar los valores de la Tabla 31 15 en 2 dimensiones, por lado la dimensión impacto, y por otro lado la dimensión compuesta por la probabilidad, la habilidad y el costo, se obtiene la Tabla 32.

Tabla 32 - Riesgo IOT calculado en función de probabilidad por impacto

NODO	PROBABILIDAD * HABILIDAD / COSTO	IMPACTO	RIESGO
H_A.1.1	0.3500	7.0000	2.4500
H_A.1.2	0.3250	7.0000	2.2750
H_A.2	0.3500	8.0000	2.8000
H_A.3	0.3250	9.0000	2.9250
H_A.4.1	0.3500	8.0000	2.8000
H_A.4.2	0.4500	8.0000	3.6000
H_A.4.3	0.2500	8.0000	2.0000
H_A.4.4	0.4500	8.0000	3.6000
H_A.4.5	0.1500	9.0000	1.3500
H_B.1.1	0.3000	7.0000	2.1000
H_B.1.2	0.3000	8.0000	2.4000
H_B.2.1	0.4500	7.0000	3.1500
H_B.2.2	0.4000	8.0000	3.2000
H_B.3	0.3250	9.0000	2.9250
H_B.4	0.3500	9.0000	3.1500
O_A.1	0.1138	9.1000	1.0351
O_A.4	0.42830	9.0000	3.8547
O_B.1	0.0900	9.4000	0.8460
O_B.2	0.4900	8.0000	3.9200
O_A	0.4093	9.1000	3.7246
O_B	0.440422	9.4000	4.1400
O_T	0.42452	9.4000	3.9905

Los valores obtenidos del atributo riesgo de cada nodo corresponden al riesgo inherente, debido a que en el árbol aún no se proponen controles de seguridad para reducir el riesgo. Siendo el riesgo inherente total del árbol, el correspondiente al nodo OT, mismo que posee un valor de 2.9717.

Para realizar un análisis más visual de estos valores, siguiendo un método similar al de [5] se utilizará el siguiente mapa semántico para determinar la criticidad de los riesgos registrados.

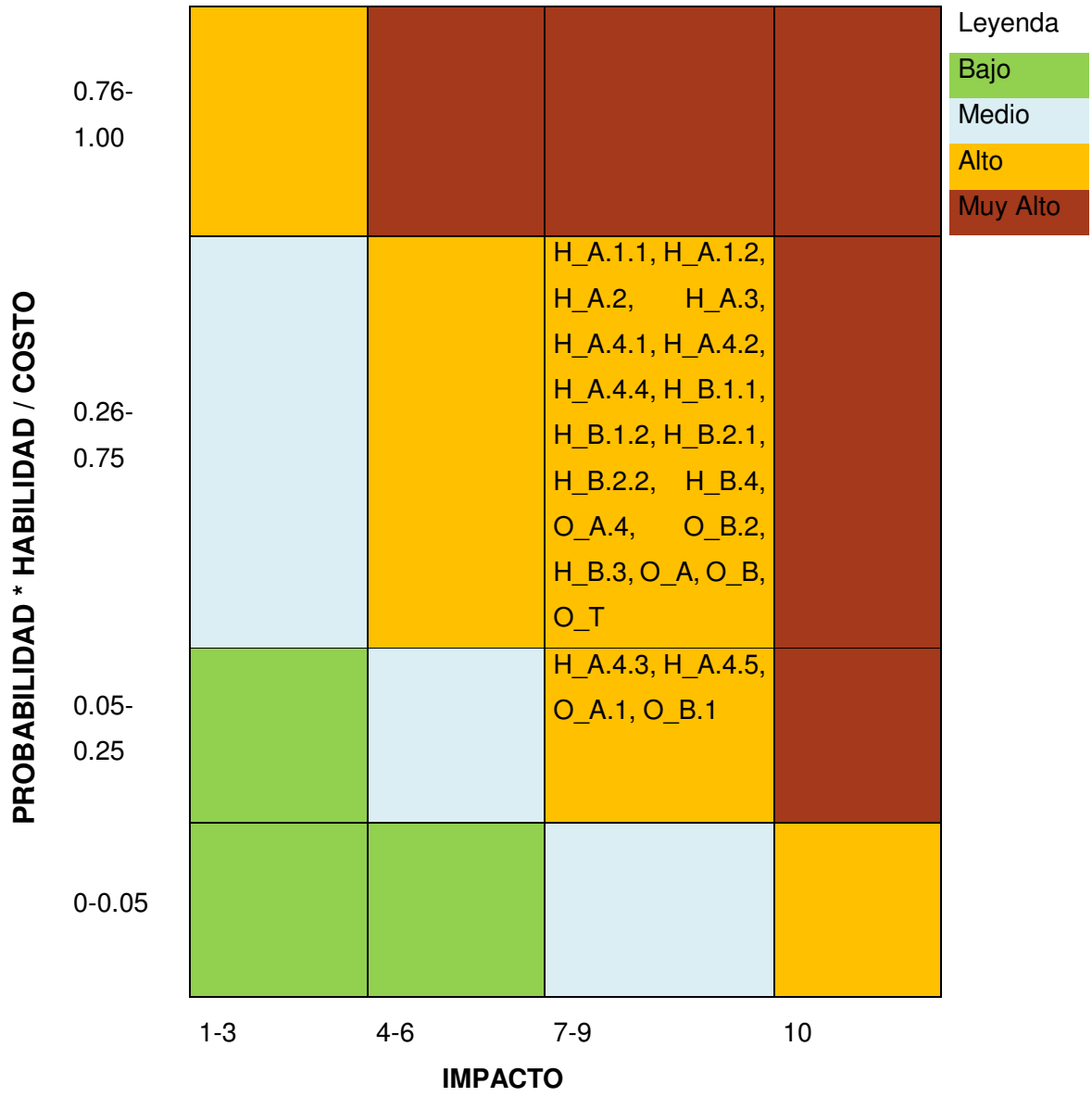


Figura 39 - Mapa semántico de riesgo inherente IOT

Se puede apreciar que todos los riesgos inherentes del árbol de ataque del caso de estudio se encuentran como Alto, siendo el riesgo inherente total, alto.

2.3 CONTROL DE RIESGOS

Como se indica en la sección “Propuesta de ciclo de gestión de riesgos” del presente trabajo, la lista de controles de seguridad que se utilizaran para la generación de los árboles de defensa se encuentra en el Anexo II y están basados en EGSI y RGPD y los controles sugeridos por [21].

2.4 TRATAMIENTO DE RIESGOS

Para tratar los riesgos encontrados en la etapa de evaluación, se propone usar arboles de defensa que utilizaran los controles de seguridad generados como contramedidas y con estos calcular el riesgo residual.

2.4.1 Diseño y creación de árboles de defensa IOT

Con el fin de realizar un análisis cuantitativo es necesario dar valores iniciales para los controles de seguridad definidos en el Anexo II, estos valores consideran como referencia el escenario de brechas.

Tabla 33 - Valores estimados por contramedida IOT

CONTRAMEDIDA	CÓDIGO	TIPO	VALOR	COSTO	VALOR FINAL
Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	C3	Probabilidad	A 0.80	M 2	0.40
Establecer controles para la protección contra código malicioso.	C4	Probabilidad	A 0.80	B 1	0.80
Establecer reglas de control de acceso.	C5	Probabilidad	M 0.75	B 1	0.75

En la siguiente Tabla se presentan las contramedidas sustentadas en los controles de seguridad del Anexo II y su aplicación en los nodos seleccionados.

Tabla 34 - Contramedidas por nodo seleccionado IOT

CÓDIGO NODO	DESCRIPCIÓN NODO	CÓDIGO CONTRAMEDIDA
H_A.1.1	Escuchar e interferir con la comunicación entre dispositivo y Gateway	C3
H_A.1.2	Rastrear tráfico del cliente móvil.	C3
H_A.2	Explotar servicios no usados	C3
H_A.3	Ejecutar código no autorizado	C4
H_A.4.1	Obtener acceso a datos de registro	C5
H_A.4.2	Obtener acceso por interfaz	C5
H_A.4.3	Extraer clave cifrada	C3
H_A.4.4	Usar claves predeterminadas	C3
H_A.4.5	Falsificar dispositivo	C3
H_B.1.1	Revertir contenido cifrado	C3
H_B.1.2	Extraer clave cifrada	C3
H_B.2.1	Obtener acceso por la interfaz	C5
H_B.2.2	Reusar tokens de un dispositivo en otro	C5
H_B.3	Ejecutar código no autorizado	C4
H_B.4	Explotar vulnerabilidades conocidas	C3

2.4.2 Generación de árboles de defensa IOT

En base al árbol de ataque IOT y a los controles de seguridad definidos. mediante la herramienta ADTool, se genera el correspondiente árbol de defensa [30]:

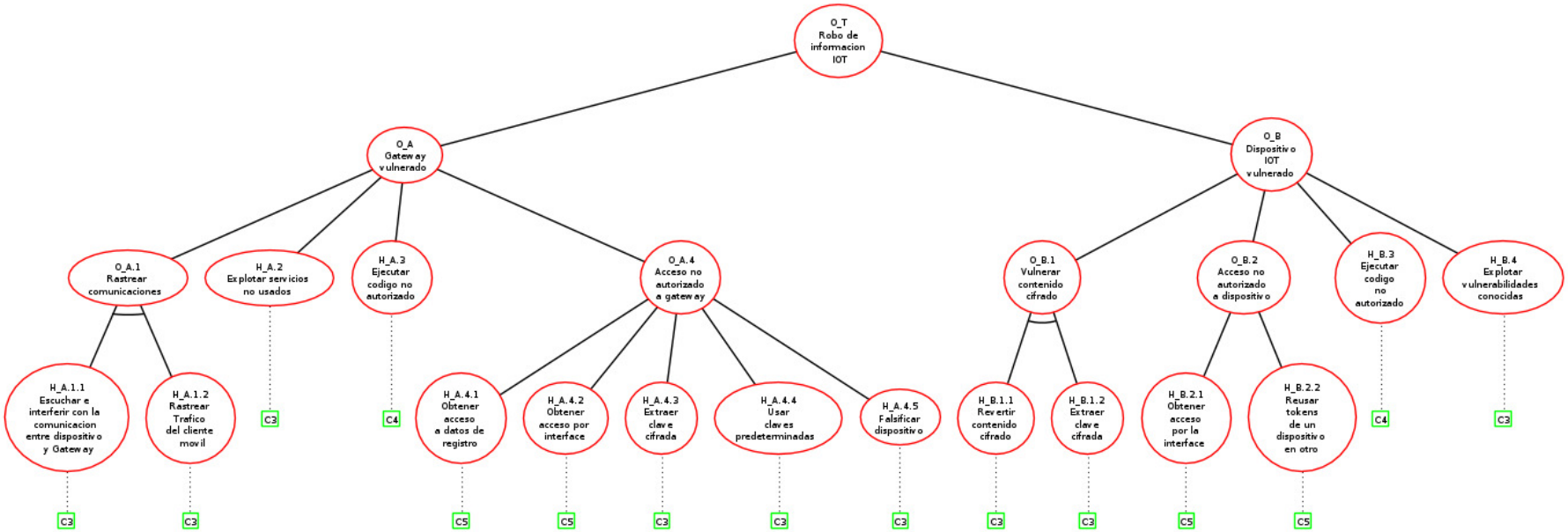


Figura 40 - Árbol de defensa "Robo de información IOT"

2.3.3 Definición valores iniciales para nodos hoja usando contramedidas IOT

Usando los valores tipo hoja de la Tabla 30 y los valores de las contramedidas asignados en la Tabla 34, se pueden obtener los valores de los atributos de los nodos tipo hoja del árbol de defensa.

Tabla 35 - Valores de atributos iniciales del árbol de defensa “Robo de información IOT”

CÓDIGO	COSTO	IMPACTO	HABILIDAD	PROBABILIDAD	RIESGO	CONTRAMEDIDA	VALOR DE CONTRAMEDIDA	COSTO FINAL	IMPACTO FINAL	HABILIDAD FINAL	PROBABILIDAD FINAL	RIESGO FINAL
H_A.1.1	1.0000	7.0000	0.5000	0.7000	2.4500	C3	0.4000	1.0000	7.0000	0.5000	0.4200	1.4700
H_A.1.2	1.0000	7.0000	0.5000	0.6500	2.2750	C3	0.4000	1.0000	7.0000	0.5000	0.3900	1.3650
H_A.2	1.0000	8.0000	0.5000	0.7000	2.8000	C3	0.4000	1.0000	8.0000	0.5000	0.4200	1.6800
H_A.3	1.0000	9.0000	0.5000	0.6500	2.9250	C4	0.8000	1.0000	9.0000	0.5000	0.1300	0.5850
H_A.4.1	1.0000	8.0000	0.5000	0.7000	2.8000	C5	0.7500	1.0000	8.0000	0.5000	0.1750	0.7000
H_A.4.2	1.0000	8.0000	0.5000	0.9000	3.6000	C5	0.7500	1.0000	8.0000	0.5000	0.2250	0.9000
H_A.4.3	1.0000	8.0000	0.5000	0.5000	2.0000	C3	0.4000	1.0000	8.0000	0.5000	0.3000	1.2000
H_A.4.4	1.0000	8.0000	0.5000	0.9000	3.6000	C3	0.4000	1.0000	8.0000	0.5000	0.5400	2.1600
H_A.4.5	2.0000	9.0000	0.5000	0.6000	1.3500	C3	0.4000	2.0000	9.0000	0.5000	0.3600	0.8100
H_B.1.1	1.0000	7.0000	0.5000	0.6000	2.1000	C3	0.4000	1.0000	7.0000	0.5000	0.3600	1.2600
H_B.1.2	1.0000	8.0000	0.5000	0.6000	2.4000	C3	0.4000	1.0000	8.0000	0.5000	0.3600	1.4400
H_B.2.1	1.0000	7.0000	0.5000	0.9000	3.1500	C5	0.7500	1.0000	7.0000	0.5000	0.2250	0.7875
H_B.2.2	1.0000	8.0000	0.5000	0.8000	3.2000	C5	0.7500	1.0000	8.0000	0.5000	0.2000	0.8000
H_B.3	1.0000	9.0000	0.5000	0.6500	2.9250	C4	0.8000	1.0000	9.0000	0.5000	0.1300	0.5850
H_B.4	1.0000	9.0000	0.5000	0.7000	3.1500	C3	0.4000	1.0000	9.0000	0.5000	0.4200	1.8900

Para una mejor compresión de la Tabla 35, se ejemplifica el cálculo de los nuevos valores de atributos para el nodo H_A.1.1

Costo final H_A.1.1 = Costo H_A.1.1

Costo final H_A.1.1 = 1

Impacto final H_A.1.1 = Impacto H_A.1.1 (No existe contramedida de impacto)

Impacto final H_A.1.1 = 7

Habilidad final H_A.1.1 = Habilidad H_A.1.1

Habilidad final H_A.1.1 = 0.50

Probabilidad final H_A.1.1 = Probabilidad H_A.1.1 x (1 – Probabilidad Contramedida C3))

Probabilidad final H_A.1.1 = 0.70 x (1 – 0.40)

Probabilidad final H_A.1.1 = 0.70 x (0.60)

Probabilidad final H_A.1.1 = 0.42

Riesgo final H_A.1.1 = $\frac{(\text{Probabilidad H\_A.1.1x Impacto H\_A.1.1 x Habilidad H\_A.1.1})}{Costo\ \text{H\_A.1.1}}$

Riesgo final H_A.1.1 = $\frac{(0.42 \text{ x } 7 \text{ x } 0.50)}{1}$

Riesgo final H_A.1.1 = 1.47

2.4.4 Propagación de valores en el árbol de defensa IOT

Previo al cálculo del riesgo residual es necesario propagar los atributos por todos los nodos del árbol de defensa. Para conseguir este objetivo, se utilizarán las fórmulas de la Tabla 13 y Tabla 18, en conjunto con los valores de la Tabla 33 y Tabla 35, para obtener los siguientes resultados.

Tabla 36 - Propagación de atributos por el árbol de defensa “Robo de información IOT”

CÓDIGO	COSTO	IMPACTO	HABILIDAD	PROBABILIDAD	RIESGO	CONTRAMEDIDA	VALOR DE CONTRAMEDIDA	COSTO FINAL	IMPACTO FINAL	HABILIDAD FINAL	PROBABILIDAD FINAL	RIESGO FINAL
H_A.1.1	1.0000	7.0000	0.5000	0.7000	2.4500	C3	0.4000	1.0000	7.0000	0.5000	0.4200	1.4700
H_A.1.2	1.0000	7.0000	0.5000	0.6500	2.2750	C3	0.4000	1.0000	7.0000	0.5000	0.3900	1.3650
H_A.2	1.0000	8.0000	0.5000	0.7000	2.8000	C3	0.4000	1.0000	8.0000	0.5000	0.4200	1.6800
H_A.3	1.0000	9.0000	0.5000	0.6500	2.9250	C4	0.8000	1.0000	9.0000	0.5000	0.1300	0.5850
H_A.4.1	1.0000	8.0000	0.5000	0.7000	2.8000	C5	0.7500	1.0000	8.0000	0.5000	0.1750	0.7000
H_A.4.2	1.0000	8.0000	0.5000	0.9000	3.6000	C5	0.7500	1.0000	8.0000	0.5000	0.2250	0.9000
H_A.4.3	1.0000	8.0000	0.5000	0.5000	2.0000	C3	0.4000	1.0000	8.0000	0.5000	0.3000	1.2000
H_A.4.4	1.0000	8.0000	0.5000	0.9000	3.6000	C3	0.4000	1.0000	8.0000	0.5000	0.5400	2.1600
H_A.4.5	2.0000	9.0000	0.5000	0.6000	1.3500	C3	0.4000	2.0000	9.0000	0.5000	0.3600	0.8100
H_B.1.1	1.0000	7.0000	0.5000	0.6000	2.1000	C3	0.4000	1.0000	7.0000	0.5000	0.3600	1.2600
H_B.1.2	1.0000	8.0000	0.5000	0.6000	2.4000	C3	0.4000	1.0000	8.0000	0.5000	0.3600	1.4400
H_B.2.1	1.0000	7.0000	0.5000	0.9000	3.1500	C5	0.7500	1.0000	7.0000	0.5000	0.2250	0.7875
H_B.2.2	1.0000	8.0000	0.5000	0.8000	3.2000	C5	0.7500	1.0000	8.0000	0.5000	0.2000	0.8000
H_B.3	1.0000	9.0000	0.5000	0.6500	2.9250	C4	0.8000	1.0000	9.0000	0.5000	0.1300	0.5850
H_B.4	1.0000	9.0000	0.5000	0.7000	3.1500	C3	0.4000	1.0000	9.0000	0.5000	0.4200	1.8900
O_A.1	2.0000	9.1000	0.5000	0.4550	1.0351	-	-	2.0000	9.1000	0.5000	0.1638	0.3726
O_A.4	1.1667	9.0000	0.5000	0.9994	3.8547	-	-	1.2250	9.0000	0.5000	0.8682	3.1894
O_B.1	2.0000	9.4000	0.5000	0.3600	0.8460	-	-	2.0000	9.4000	0.5000	0.1296	0.3046
O_B.2	1.0000	8.0000	0.5000	0.9800	3.9200	-	-	1.0000	8.0000	0.5000	0.3800	1.5200
O_A	1.2216	9.1000	0.5000	1.0000	3.7246	-	-	1.2270	9.1000	0.5000	0.9444	3.5020
O_B	1.1338	9.4000	0.5000	0.9987	4.1400	-	-	1.1223	9.4000	0.5000	0.7277	3.0474
O_T	1.1778	9.4000	0.5000	1.0000	3.9905	-	-	1.1815	9.4000	0.5000	0.9849	3.9179

2.4.5 Cálculo y valoración del riesgo residual IOT

Al trabajar los valores de la Tablas 36 en 2 dimensiones, por lado la dimensión impacto, y por otro lado la dimensión compuesta por la probabilidad, la habilidad y el costo, se obtiene la Tabla 37.

Tabla 37 - Riesgo calculado en función de probabilidad por impacto para el árbol de defensa "Robo de información IOT"

NODO	PROBABILIDAD * HABILIDAD / COSTO	IMPACTO	RIESGO
H_A.1.1	0.2100	7.0000	1.4700
H_A.1.2	0.1950	7.0000	1.3650
H_A.2	0.2100	8.0000	1.6800
H_A.3	0.0650	9.0000	0.5850
H_A.4.1	0.0875	8.0000	0.7000
H_A.4.2	0.1125	8.0000	0.9000
H_A.4.3	0.1500	8.0000	1.2000
H_A.4.4	0.2700	8.0000	2.1600
H_A.4.5	0.0900	9.0000	0.8100
H_B.1.1	0.1800	7.0000	1.2600
H_B.1.2	0.1800	8.0000	1.4400
H_B.2.1	0.1125	7.0000	0.7875
H_B.2.2	0.1000	8.0000	0.8000
H_B.3	0.0650	9.0000	0.5850
H_B.4	0.2100	9.0000	1.8900
O_A.1	0.0410	9.1000	0.3726
O_A.4	0.3544	9.0000	3.1894
O_B.1	0.0324	9.4000	0.3046
O_B.2	0.1900	8.0000	1.5200
O_A	0.3848	9.1000	3.5020
O_B	0.3242	9.4000	3.0474
O_T	0.4168	9.4000	3.9179

Los valores obtenidos del atributo riesgo de cada nodo corresponden al riesgo residual, debido a que el árbol ya considera controles de seguridad basados que buscan proteger la información sensible para reducir el riesgo. Siendo el riesgo residual total del árbol, el correspondiente al nodo OT, mismo que posee un valor de 3.91.

Para realizar un análisis más visual de estos valores, siguiendo un método similar al de [5] se utilizará el siguiente mapa semántico para determinar la criticidad de los riesgos registrados.

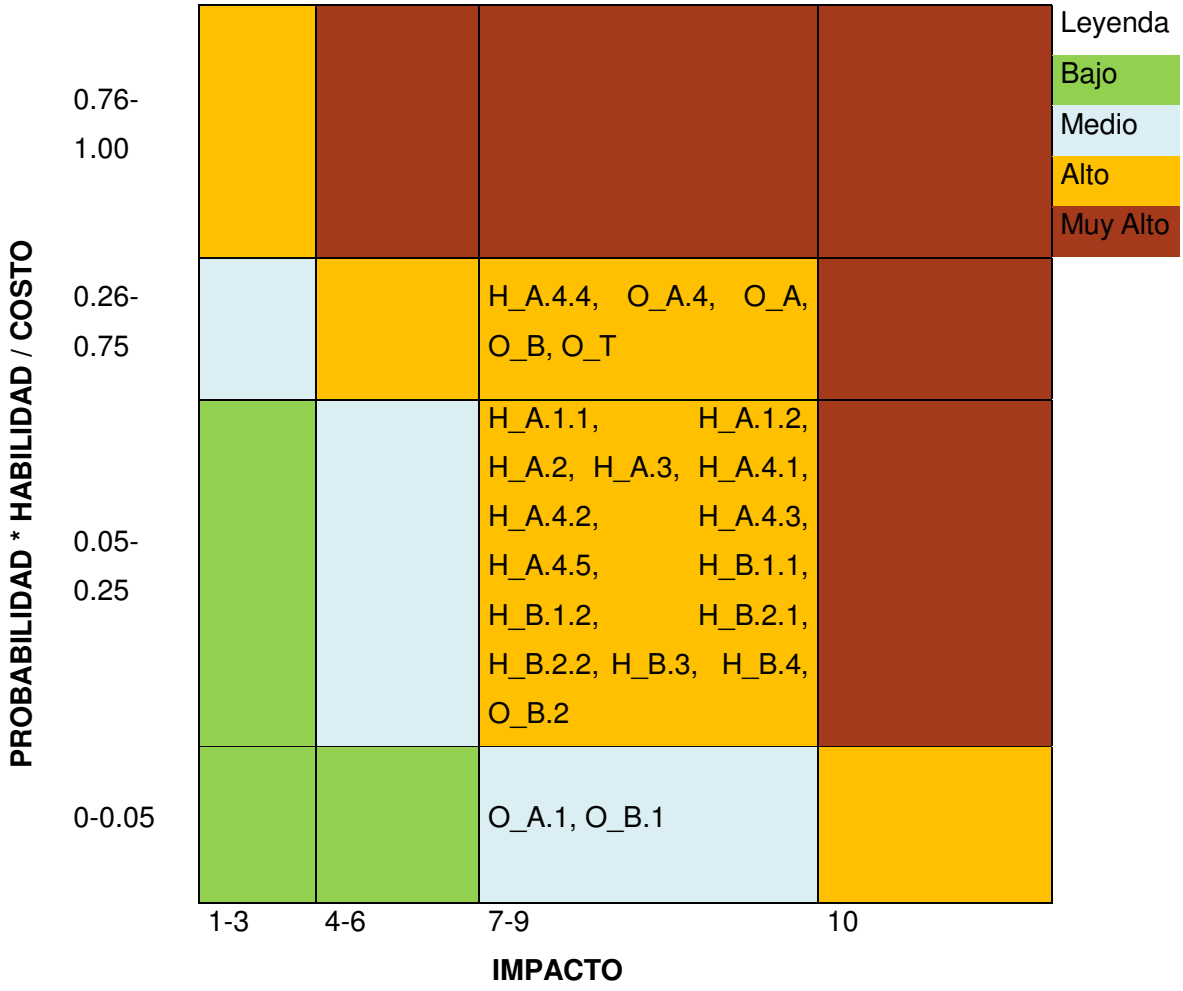


Figura 41 - Mapa semántico de riesgo residual IOT

Una vez aplicados los controles de seguridad propuestos, Se puede apreciar que todos los riesgos residuales del árbol de defensa del caso de estudio, reducido sus probabilidades, sin embargo, aún se mantienen como altos y medios, es importante indicar el hecho de que el riesgo residual total se mantiene como Alto.

2.5 COMUNICACIÓN Y VALIDACIÓN

Para validar y realizar la comunicación dentro del ciclo es necesario comparar los riesgos: inherente y residual, con esto se puede analizar la efectividad de los controles propuestos

2.5.1 Comparación entre riesgos IOT

El análisis cualitativo de los mapas semánticos utilizados en las figuras 39 y 41, permite apreciar que la implantación de controles de seguridad enfocados en la privacidad reduce considerablemente la probabilidad de su manifestación en los nodos hoja, sim embargo el impacto se mantiene.

Para completar el análisis cualitativo realizado, es necesario realizar un análisis de índole cuantitativa, y con este fin, apoyado en el trabajo de [5] se utilizará una variante de la ficha de informes de riesgos, que permitan comparar los riesgos residuales e inherentes para el presente caso de estudio.

Tabla 38 - Ficha comparativa de riesgos inherente y residual IOT

				RIESGO INHERENTE			RIESGO RESIDUAL			
Código Riesgo	**Descripción del Riesgo**	**Descripción Control**	**Tipo Control**	**Probabilidad**	**Impacto**	**Riesgo**	**Probabilidad**	**Impacto**	**Riesgo**	**% Reducción**
H_A.1.1	Escuchar e interferir con la comunicación entre dispositivo y Gateway	Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	Probabilidad	0.3500	7.0000	2.4500	0.2100	7.0000	1.4700	40.00
H_A.1.2	Rastrear tráfico del cliente móvil.	Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	Probabilidad	0.3250	7.0000	2.2750	0.1950	7.0000	1.3650	40.00
H_A.2	Explotar servicios no usados	Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	Probabilidad	0.3500	8.0000	2.8000	0.2100	8.0000	1.6800	40.00
H_A.3	Ejecutar código no autorizado	Establecer controles para la protección contra	Probabilidad	0.3250	9.0000	2.9250	0.0650	9.0000	0.5850	80.00

				RIESGO INHERENTE			RIESGO RESIDUAL			
Código Riesgo	**Descripción del Riesgo**	**Descripción Control**	**Tipo Control**	**Probabilidad**	**Impacto**	**Riesgo**	**Probabilidad**	**Impacto**	**Riesgo**	**% Reducción**
		código malicioso.								
H_A.4.1	Obtener acceso a datos de registro	Establecer reglas de control de acceso.	Probabilidad	0.3500	8.0000	2.8000	0.0875	8.0000	0.7000	75.00
H_A.4.2	Obtener acceso por interfaz	Establecer reglas de control de acceso.	Probabilidad	0.4500	8.0000	3.6000	0.1125	8.0000	0.9000	75.00
H_A.4.3	Extraer clave cifrada	Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	Probabilidad	0.2500	8.0000	2.0000	0.1500	8.0000	1.2000	40.00
H_A.4.4	Usar claves predeterminadas	Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	Probabilidad	0.4500	8.0000	3.6000	0.2700	8.0000	2.1600	40.00
H_A.4.5	Falsificar dispositivo	Establecer estándares de configuración segura,	Probabilidad	0.1500	9.0000	1.3500	0.0900	9.0000	0.8100	40.00

				RIESGO INHERENTE			RIESGO RESIDUAL			
Código Riesgo	**Descripción del Riesgo**	**Descripción Control**	**Tipo Control**	**Probabilidad**	**Impacto**	**Riesgo**	**Probabilidad**	**Impacto**	**Riesgo**	**% Reducción**
		desarrollo y actualización de los sistemas.								
H_B.1.1	Revertir contenido cifrado	Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	Probabilidad	0.3000	7.0000	2.1000	0.1800	7.0000	1.2600	40.00
H_B.1.2	Extraer clave cifrada	Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	Probabilidad	0.3000	8.0000	2.4000	0.1800	8.0000	1.4400	40.00
H_B.2.1	Obtener acceso por la interfaz	Establecer reglas de control de acceso.	Probabilidad	0.4500	7.0000	3.1500	0.1125	7.0000	0.7875	75.00
H_B.2.2	Reusar tokens de un dispositivo en otro	Establecer reglas de control de acceso.	Probabilidad	0.4000	8.0000	3.2000	0.1000	8.0000	0.8000	75.00
H_B.3	Ejecutar código no autorizado	Establecer controles para la	Probabilidad	0.3250	9.0000	2.9250	0.0650	9.0000	0.5850	80.00

				RIESGO INHERENTE			RIESGO RESIDUAL			
Código Riesgo	**Descripción del Riesgo**	**Descripción Control**	**Tipo Control**	**Probabilidad**	**Impacto**	**Riesgo**	**Probabilidad**	**Impacto**	**Riesgo**	**% Reducción**
		protección contra código malicioso.								
H_B.4	Explotar vulnerabilidades conocidas	Establecer estándares de configuración segura, desarrollo y actualización de los sistemas.	Probabilidad	0.3500	9.0000	3.1500	0.2100	9.0000	1.8900	40.00
O_A.1	Rastrear comunicaciones			0.1138	9.1000	1.0351	0.0410	9.1000	0.3726	64.00
O_A.4	Acceso no autorizado a Gateway			0.42830	9.0000	3.8547	0.3544	9.0000	3.1894	17.26
O_B.1	Vulnerar contenido cifrado			0.0900	9.4000	0.8460	0.0324	9.4000	0.3046	64.00
O_B.2	Acceso no autorizado a dispositivo			0.4900	8.0000	3.9200	0.1900	8.0000	1.5200	61.22
O_A	Gateway vulnerado			0.4093	9.1000	3.7246	0.3848	9.1000	3.5020	5.97
O_B	Dispositivo IOT vulnerado			0.440422	9.4000	4.1400	0.3242	9.4000	3.0474	26.38
O_T	Robo de información IOT			0.42452	9.4000	3.9905	0.4168	9.4000	3.9179	1.82

2.5.2 Análisis de efectividad IOT

En base al trabajo realizado en la ficha comparativa de riesgos inherente y residual se puede aprecia que:

El riesgo inherente generado por ataques que roban información personal sensible tiene un impacto muy alto, que afecta considerablemente la privacidad de los usuarios de los sistemas de información afectados por este tipo de brechas.

Los controles de seguridad orientados a salvaguardar la privacidad de la información aplicados en un ambiente de IOT ayudan a reducir significativamente la probabilidad en los nodos hoja de los ataques, este hecho se evidencia al revisar los riesgos reportados en la ficha comparativa. Se debe indicar que en ambientes IOT los controles de seguridad basado en la privacidad no son suficientes por sí solos.

Con el uso de los mapas semánticos se apreció una reducción de riesgo conservadora, mediante la comparación cuantitativa se puede observar que la reducción del riesgo varía entre el 5 y 80% en todos los riesgos que tienen implementados una contramedida basada en la protección de los datos sensibles personales.

2.6 MONITOREO

Considerando los valores de reducción evidenciados en la “Ficha comparativa de riesgos inherente y residual IOT”, se puede decir que la implementación controles de seguridad basados en EGSI y RGPD para la protección de la privacidad de datos personales sensibles son insuficientes en la gestión de riesgos de los sistemas de información IOT. Se recomendaría un nuevo ciclo de gestión con nuevos controles.

Anexo VIII - Guía simple de implementación

Para la implementación del ciclo de gestión de riesgos propuestos es necesario considerar las etapas de este.

- Establecer contexto.
- Evaluación de riesgos.
- Control de riesgos.
- Tratamiento de riesgos.
- Comunicación y valoración.
- Monitoreo.

A continuación, se expone las actividades a realizar en cada etapa.

Establecer contexto

En esta fase se debe definir de manera adecuada el escenario bajo el cual la organización está siendo afectada por las diversas brechas o eventos de seguridad.

Para conseguir este objetivo se debe realzar las siguientes tareas:

- Modelar el sistema. - consiste en determinar la infraestructura organizacional, tanto en *hardware*, *software* y personas que interactúan. Con este fin es necesario observar con atención la empresa en la cual se está implementando el ciclo de gestión.
- Modelar ataque. - consiste en determinar la manera en que la infraestructura ha sido vulnerada por uno o varios ataques.
- Perfil de atacantes. - consiste en definir los distintos grupos que han hecho mal uso de la infraestructura buscando ocasionar daño a la organización. En esta fase se debe considerar, la habilidad, el presupuesto y el tiempo del cual disponen estos grupos.
- Catálogo de amenazas. - consiste en definir el conjunto de amenazas que afectan la infraestructura organizacional, para obtener este catálogo se hace uso de la herramienta *Microsoft Thread Modeling Tool,* la misma que permite obtener esta información en base a la infraestructura tecnológica de la organización.

Evaluación de riesgos

Con el contexto establecido de manera adecuada, se puede evaluar los riesgos, para esto se debe:

- Generar árboles de ataque. - con el uso de la herramienta ADTool y con el catálogo de amenazas se puede diseñar y crear los árboles de ataque que ha sufrido la

organización. Es importante considerar el objetivo principal de estos ataques, por ejemplo, el robo de información sensible.

- Definición de atributos y valores para los nodos hoja. - en esta fase es necesario en primer lugar definir que atributos se utilizaran para caracterizar los riesgos, como mínimo se sugiere utilizar probabilidad e impacto, atributos que maneja la herramienta ADTool. Otra consideración fundamental dentro de esta fase es la asignación de valores para cada nodo del árbol de ataque, para realizar esta actividad es necesario usar el juicio experto de los actores afectados por los diversos ataques.
- Propagación de valores. - esta fase consiste en realizar el cálculo para cada nodo superior del árbol, para subir los valores de los atributos considerados, es importantes indicar que ADTool, permite realizar estos cálculos de manera automática para determinados atributos como la probabilidad.
- Cálculo y valoración del riesgo inherente. – en esta fase es necesario calcular el riesgo para cada nodo del árbol de ataque, considerando que una de las maneras de valorar el riesgo es mediante el uso de la fórmula, **riesgo = probabilidad x impacto**. Una vez valorado es riesgo se recomienda sumariar el mismo en una tabla y un mapa semántico o de calor para calificar estos riesgos.

Control de riesgos

Con el riesgo inherente valorado, es necesario establecer los controles que pueden ayudar a mitigar los mismos.

Tratamiento de riesgos

Una vez definidos los controles a utilizar, es necesario tratar los riesgos encontrados para esto se propone realizar las siguientes actividades:

- Generación de árboles de defensa. - con el uso de la herramienta ADTool y con el uso del catálogo de amenazas y los controles de seguridad determinados, se puede diseñar y crear los árboles de defensa.
- Definición de atributos y valores para los nodos hoja usando contramedidas. - en esta fase es necesario en primer lugar definir el valor que se otorgará a cada medida y que tipo de contramedidas se usa, sean de probabilidad o de impacto. Es importante anotar que los valores estimados para las contramedidas se obtienen en base a un juicio experto de la persona o personas que realizan la gestión del riesgo.

- Propagación de valores. - esta fase consiste en realizar el cálculo para cada nodo superior del árbol, para subir los valores de los atributos considerados, es importantes indicar que ADTool, permite realizar estos cálculos de manera automática para determinados atributos como la probabilidad.
- Cálculo y valoración del riesgo residual. – en esta fase es necesario calcular el riesgo residual para cada nodo del árbol de defensa, considerando que una de las maneras de valorar el riesgo es mediante el uso de la fórmula, **riesgo = probabilidad x impacto**. Una vez valorado es riesgo se recomienda sumariar el mismo en una tabla y un mapa semántico o de calor para calificar estos riesgos.

Comunicación y validación

Con los riesgos residual e inherentes cálculos, es necesario validar estos y comunicar los resultados, para cumplir este objetivo es necesario realizar las siguientes actividades.

Comparar riesgos. – se recomienda crear una ficha comparativa de los riesgos inherente y residual, que contenga al menos el nombre de la amenaza, la contramedida usada, el riesgo, y la diferencia porcentual entre estos.

Análisis de efectividad. - en este paso es necesario con la tabla generada analizar si las contramedidas han trabajado de manera adecuada, verificando si el riesgo ha disminuido y en que valores, es especial el riesgo total del ataque.

Monitoreo

En esta etapa final, es necesario con los datos recolectados, determinar la efectividad del ciclo, y definir se es necesario entrar en una nueva etapa inicial, o se procede a aceptar el riesgo residual resultante.