UNIVERSIDAD SIMÓN BOLÍVAR
BARRANQUILLA Y CÚCUTA - COLOMBIA
VIGILADA MINEDUCACIÓN

Res. 23095, del MEN

# PROPUESTA METODOLÓGICA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA DE INFORMACIÓN FÉNIX DE LA CLÍNICA BONNADONA PREVENIR


**Elaborado por:**

**ING. CABALLERO VILLAMIL BRIAN**

**ING. LLANOS ÁLVAREZ JEISON JOSE**

**ING. SALGADO CASTRO CAMILO**


**Presentado a:**

**UNIVERSIDAD SIMÓN BOLÍVAR**

**PROGRAMA ESP. GESTIÓN DE TI**

**Barranquilla, 16 de noviembre del 2020**

**CONTENIDO**

# 1 PRESENTACIÓN DEL CASO.

## 1.1 Resumen o semblanza del estudio de caso

El presente estudio de caso se desarrollará para generar una propuesta metodológica para la gestión de riesgos asociados a la seguridad de la información en el proyecto de software de seguridad del paciente ***Fénix,*** desarrollado por el área de software de la Organización Clínica Bonnadona Prevenir, basada en el marco de trabajo COBIT 5, las normativas NTC ISO/IEC 27001, NTC ISO/IEC 27005, y los criterios seleccionados del estándar OWASP que van enfocadas a la identificación, la gestión, la evaluación y mitigación de causas de riesgos.

Si bien la organización cuenta con un departamento de calidad encargado de la gestión de riesgos para todas las áreas, este no ha identificado los riesgos asociados a los proyectos de software desarrollados en la organización.

Las empresas del sector salud necesitan estar vinculadas a las tecnologías de la información de forma muy estrecha, mitigar las causas de los riesgos es un trabajo de vital importancia para la organización; Sin embargo, se evidenció que no existe una metodología definida que permita gestionar de seguridad de la información del software ***Fénix***.

La búsqueda de metodologías adecuadas para contener los riesgos asociados al área de software de la organización ha propiciado una generación de cambios tanto en herramientas tecnológicas, recursos humanos, y otros agentes que son de gran impacto.

La gestión de riesgos del proyecto de desarrollo de software de seguridad del paciente debe centrarse en la reducción y prevención de eventos de seguridad asociados a la data de las historias clínicas, permitiendo evaluar continuamente las inconsistencias, integridad y calidad de información que a su vez conlleva a determinar qué riesgos están presentes, su categorización y

tratamiento. La materialización de algunos de los riesgos encontrados durante la etapa de identificación, pueden afectar de forma considerable el proyecto, tanto económicamente como en el activo de tiempo. También se deben tener en cuenta las multas o acciones legales que se pueden llevar contra la organización por el incumplimiento del tratamiento de datos personales y que finalmente afectarían su imagen, que impactaría negativamente a nivel operativo y estratégico.

La Organización Clínica Bonnadona Prevenir, desde hace un par de años ha venido incursionando en proyectos de software bajo arquitectura web, lo cual permite que este sea accesible incluso fuera de las instalaciones de la organización. En la mayoría de los proyectos de desarrollo de software, las causas más probables de los riesgos son: el uso de tecnologías nuevas y no probadas, requisitos del sistema, arquitectura del sistema, rendimiento del sistema y asuntos organizacionales o no funcionales (Tao, 2008).

> Según Sergey Avdoshin en su artículo, la tasa de fracaso para los proyectos de software se ha mantenido básicamente durante los últimos 15 años, en más del 40% al 50%, a pesar de los diferentes métodos de gestión, nuevas tecnologías y herramientas innovadoras que han surgido en el transcurso del tiempo (Avdoshin & Pesotskaya, 2011, p. 1).

Por lo anterior, se pensó en la forma de organizar el proceso de desarrollo de proyectos de software, por lo cual es necesario, aplicar una metodología de gestión de riesgos desde el diseño, alineados con las tendencias tecnológicas y a los retos que debe enfrentar la clínica en cuanto a seguridad del paciente y su información.

La gestión de riesgos se considera uno de los principales factores que influyen en el éxito de los proyectos. El levantamiento de la situación actual basado en la experiencia, capacidad de los gestores de riesgos e implicados en el proyecto aportará valor al resultado esperado en el software requerido fortaleciendo la seguridad desde el diseño.

Se buscará implementar una metodología que se adapte inicialmente al proyecto de software de seguridad del paciente ***Fénix***, pero que aplique al resto de los proyectos que se planeen en la organización. Se indagará sobre metodologías y estándares de gestión de riesgos ya aplicados con el fin de determinar los puntos favorables y seleccionables para esta propuesta.

## 1.2 Contextualización del problema y descripción de la unidad de análisis (diacronía):

La **Organización Clínica Bonnadona Prevenir** es una IPS que brinda servicios de salud de mediana y alta complejidad con énfasis en Hemato-oncología, que busca garantizar la seguridad del paciente, la humanización, la gestión de riesgos y el compromiso con los colaboradores (H., 2015). Dentro de su plan estratégico, destaca al departamento de TI con la innovación tecnológica, el desarrollo e implementación de software, la prestación de otros servicios de TI y la gestión de los riesgos.

La búsqueda de metodologías adecuadas para contener los riesgos asociados al área de desarrollo de proyectos de software ha propiciado una generación de cambios tanto en herramientas tecnológicas, recursos humanos, y otros agentes que son de gran impacto en los procesos, con esto, se desea abordar la propuesta basado en el marco de trabajo COBIT 5 y otros marcos de referencia como las normas NTC ISO/IEC 27001 para la seguridad y privacidad de la

información, de igual forma la norma ISO/IEC 27005, el estándar OWASP entre otros que serán de gran ayuda para desarrollar este trabajo.

El desarrollo e implementación de proyectos de software para las entidades del sector salud, debe llevar consigo el complimiento del conjunto de normativas legales que surgen de la necesidad de proteger el activo de información que posee la organización. En 2012 el gobierno nacional mediante la ley 1581, regula el derecho fundamental de *Habeas Data* con la finalidad de proteger los datos personales registrados en cualquier base de datos que permita realizar operaciones como recolección, almacenamiento, uso y tratamiento por parte de las entidades de naturaleza pública y/o privada (COLOMBIA, 2012).

Teniendo en cuenta la apreciación anterior, la organización debe fijar reglas de protección, medios de control y una regulación concreta para el manejo y tratamiento de los datos personales tanto del cliente interno como el externo, lo cual se convierte en unos de los principales riesgos a tratar y evaluar de forma constante, por lo tanto, obliga potencialmente a la organización a tener un modelo consistente de identificación, gestión, evaluación y tratamiento de los riesgos asociados al software ***Fénix***.

Actualmente la Organización Clínica Bonnadona Prevenir, cuenta con un departamento de calidad encargado de asegurar el cumplimiento del conjunto de políticas definidas, así mismo, con la identificación, gestión, evaluación y tratamiento de los riesgos en los diferentes departamentos que conforman esta unidad. La verificación constante de la evolución de los objetivos dentro de los plazos previstos y de los recursos que fueron asignados para dichos objetivos, hace de este departamento muy importante, sin embargo, no profundiza cuando se trata de tecnologías de la información y proyectos de software. En base a lo anterior, los riesgos

identificados en la matriz creada por el departamento de calidad, no se alinean a los específicos del área de desarrollo de software.

Dentro de la organización el departamento de TI específicamente el área de desarrollo de software es la encargada de velar por esta clase de proyectos, la cual fue creada a mediados del año 2020 por la necesidad de tener herramientas que sistematizarán algunos procesos asistenciales como el reporte de eventos adversos del paciente. Es por esto por lo que no se cuenta con la suficiente experiencia en la gestión de riesgos de seguridad, relacionándolos a la identificación, evaluación y tratamiento de los riesgos asociados a los proyectos de desarrollo de software, pensando en la seguridad de la información desde el diseño.

En el libro COBIT 5, se resalta que uno de los objetivos del gobierno de TI es reconocer un riesgo; evaluar su impacto y posibilidad de ocurrencia; y desarrollar estrategias que ayuden a mitigar dicho impacto sobre los procesos. Dado que el riesgo cero no existe para ningún caso, se requerirá que estos se evalúen exhaustivamente para evitar pérdidas, robo o corrupción de la información.

Se identificó el grupo de interesados que está directamente ligado al gobierno de TI para la gestión de los riesgos en los proyectos de software en la clínica, así:

Tabla 1.
*Actores identificados en el Gobierno de TI de la Organización Clínica Bonnadona Prevenir*

| PAPEL | DEFINICIÓN |
|---|---|
| Comité Directivo | ▪ Compuesto por la junta directiva (Gerente, subgerente) |
| Gestores de Riesgos | ▪ Departamento de Calidad (Jefe de Calidad)<br>▪ Departamento de TI |
| Jefe de Sistemas | ▪ Líder del Departamento Sistemas. |
| Coordinador de Proyectos | ▪ Líder de los proyectos de desarrollo de software |

| | |
|---|---|
| Coordinador de Aplicaciones | ▪ Líder de servicios del software |
| Líder de Proceso | ▪ Jefe del departamento de seguridad del paciente |
| Equipo de Desarrollo | ▪ Pool de desarrollo. |
| Usuario Final | ▪ Personal de la organización que usa la herramienta. |

Hoy en día la organización busca la implementación de los procesos y prácticas más actualizadas en cuanto a marco de referencia Cobit con el objetivo de alinearse a las normativas legales vigentes y al contexto estratégico organizacional. Lo anterior se debe a los cambios de enfoque que tuvo este marco de trabajo desde la versión 4.1 a la versión 5, que pasó de ser una herramienta para auditar, a un marco de visión integral de gobierno, administración y operación de las TI. Sin embargo, este marco de trabajo que fue construido para obtener una adecuada organización y administración aplicados a todo el ambiente de TI no es suficiente para brindar la protección requerida al activo de la información, por ello se necesita acudir a otros estándares, normativas o referencias que igualmente ofrecen "mejores prácticas" y encontrar los puntos de articulación donde se pueda fortalecer la metodología base hasta obtener una propuesta aceptable en lo relativo a salvaguardar la información, esto sin perder la esencia de ninguno de los marcos de referencia origen, es decir, será una metodología no excluyente.

Durante la investigación también se identificó que el estándar ISO/IEC 31000:2009 – Principios y directrices de gestión de riesgos, se puede aplicar a cualquier tipo de riesgo, indistintamente sea su naturaleza, tanto si tiene consecuencias positivas o negativas. Esta norma no es específicamente sobre la seguridad de la información o para los riesgos de TI. Sino que proporciona un enfoque general en apoyo a las normas de control de riesgos.

En cuanto al estándar internacional ISO 27001, diseñado por la organización internacional de estandarización – ISO y la comisión Electrónica Internacional – IEC, es un

modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar los sistemas de Gestión de la Seguridad de la información (SGSI). El objetivo del SGSI, no es eliminar riesgos de seguridad dado que estos no se podrán descartar de forma absoluta, sino de asegurar el activo de información gestionando los riesgos de la seguridad de la información permitiendo sean conocidos, asumidos, y minimizados para la organización, en este caso en el área de desarrollo de software, además, procura que estos sean documentados, sistemáticos, estructurados, con seguimiento continuo, eficiente y con gran capacidad de flexibilidad para que se adapten a los cambios significativos que se produzcan en la organización.

Si hablamos de seguridad en aplicaciones web, es necesario referenciar al proyecto abierto de seguridad en aplicaciones Web (OWASP, Open Web Application Security Project*)*, donde se establecen unos criterios de organización y una lista concisa sobre los riesgos más críticos sobre la seguridad en aplicaciones web (Foundation, 2013).

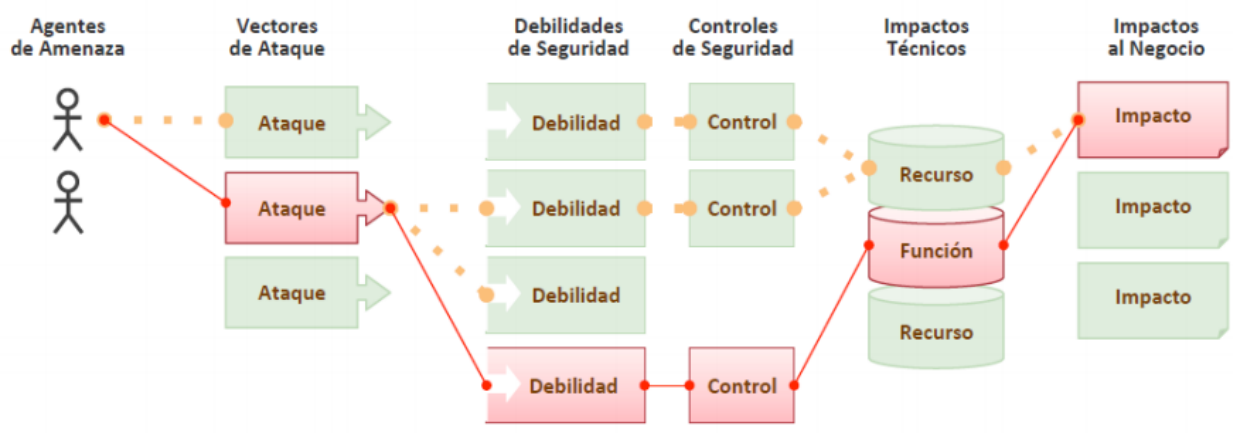


Figura 1. Representación del riesgo según estándar OWASP. Tomado de *(Foundation, 2013, p. 5)*.

En el proceso de identificación de riesgos basados en el marco de trabajo y las normativas referenciadas, se lograron identificar los activos, las amenazas, las vulnerabilidades y los requisitos legales con los que se planteará la propuesta de la gestión de riesgos asociados a la seguridad de la información del proyecto de software de seguridad del paciente ***Fénix***.

En este estudio de caso, se pretende el establecimiento de un proceso metodológico que comprenda desde la realidad de la organización y la identificación de los riesgos asociados al desarrollo de proyectos de software, hasta la implementación de un modelo de gestión, evaluación y tratamiento de riesgos inherentes a la seguridad de la información.

### 1.3 Pregunta y preguntas secundarias

Basándonos en la información recopilada y analizada, llegamos a proponer el siguiente interrogante como tema principal:

- ¿Por qué se requiere implementar herramienta de gestión de riesgo de seguridad de la información al aplicativo Fénix, basada en los estándares (NTC ISO/IEC 27001, NTC ISO/IEC 27005) y un marco de trabajo (COBIT 5)?

De igual forma se identificaron las siguientes preguntas relacionadas para confirmar el interrogante principal:

1. ¿El proyecto de seguridad del paciente fue desarrollado basado en alguna metodología?

2. ¿La gestión de riesgos para el software seguridad del paciente está orientada a cumplir con las buenas prácticas del marco de referencia OWASP?

# 2 MÉTODO

## 2.1 Determinación del método de análisis.

Teniendo en cuenta las características de este caso de estudio, y que la proyección final es el desarrollo de una propuesta metodológica para la gestión de riesgos que se pueda aplicar inicialmente en el proyecto de seguridad del paciente ***Fénix,*** y que luego se pueda implementar con los demás proyectos futuros. Se estructura el proceso fundamentado en las metas corporativas propuestas por la implementación de buenas prácticas especificadas en el marco de trabajo Cobit 5, articulados con la norma NTC ISO/IEC 27001, además, con los criterios seleccionados en el estándar OWASP en referencia a la seguridad en las aplicaciones web, dando cumplimiento a la normativa legal 1581 del 2012 de tratamiento de datos personales establecida por el gobierno nacional.

El diseño de la metodología tiene como referencia base el proceso de gestión de riesgos de seguridad de la información de la norma técnica ISO/IEC 27001 que se dividirá en 2 etapas que contienen 5 fases, donde se articularán los otros marcos referenciales destacados anteriormente, así:

- **Etapa 1, Gobierno de TI:**

En esta fase, se hace referencia al conjunto de buenas prácticas propuestas por Cobit 5 en el gobierno de TI para el establecimiento de los roles que le serán asignados a todos los involucrados en el proceso de gestión de riesgos orientados a la seguridad de la información en el software Fénix, así como la definición los lineamientos necesarios para asegurar que los procedimientos se efectúen de la forma correcta.

Como parte del gobierno, el jefe de sistemas como primer involucrado de forma directa debe definir la tolerancia de los riesgos. De esta forma, cuando se lleve a cabo el procedimiento de gestión de riesgos de seguridad de la información, se podrán tomar como referencia para la evaluación de dichos riesgos, los lineamientos establecidos por la organización, para este caso la seguridad del paciente que incluye el tratamiento responsable de su información.

- **Etapa 2, Proceso de gestión de riesgos en la seguridad de la información:**

La etapa 2 iniciaría con el proceso de gestión de riesgos en la seguridad de la información propuesto por la norma técnica ISO/IEC 27005:2008, que se articulará en las actividades establecimiento del contexto y tratamiento del riesgo con algunas mejores prácticas y actividades encontradas en los procesos catalizadores definidos en la guía de procesos de cobit 5. Es importante destacar que cada empresa tiene una cultura particular, por lo cual la aplicación de esta actividad requiere de un repensar de la organización en términos de sus necesidades (Marlene Lucila Guerrero Julio, 2019).


Figura 2. Proceso de Gestión de Riesgos en la Seguridad de la Información articulado con los diferentes marcos y estándares. Fuente: Elaboración propia.

En el establecimiento del contexto como primera actividad del proceso de gestión en la seguridad de la información, se deben considerar los factores externos o internos, las amenazas, vulnerabilidades, los diferentes tipos de riesgo, los procesos pertinentes asociados al software de seguridad del paciente ***Fénix.*** Lo anterior debe estar alineado claramente con la misión de la organización.

Si bien la mayor parte del establecimiento del contexto está relacionado con la gobernanza de TI, es necesario implementar la evaluación utilizando procesos catalizadores de Cobit. El marco de trabajo Cobit incluye 37 procesos catalizadores los cuales se constituyen en una guía para evaluar y diagnosticar el estado actual de la integración de TI en la organización en términos de gestión (Isaca, COBIT 5.0. Enabling Processes., 2012) (Isaca, COBIT 5.0. Un marco de negocio para el gobierno y la gestión de TI de la empresa, 2012).

Para llevar a cabo la primera actividad, se recomienda aplicar un instrumento para la evaluación del contexto en el área de desarrollo de software. Se propone el siguiente

instrumento de preguntas el cual fue dividido en seis dominios, para analizar el contexto de la organización en términos del desarrollo del software Fénix.

Tabla 2.
*Ejemplo de Instrumento para establecimiento del contexto articulado con COBIT*

| DOMINIO | PREGUNTA DEL INSTRUMENTO | ALINEACIÓN CON COBIT 5 |
|---|---|---|
| Plan estratégico | ¿La administración tiene claramente definida la finalidad del área de desarrollo de software?<br>¿El plan estratégico ha definido metas e indicadores de evaluación para proyectos de software?<br>¿Se han efectuado evaluaciones a los planes estratégicos? | EDM01, APO01, APO02 |
| Inversiones en Desarrollo de Software | ¿Al momento de adquirir TIC o desarrollarlas, se aplican estándares para su aprobación?<br>¿Los proyectos de TIC están vinculados al portafolio de proyectos de la organización? | APO03, BAI01, BAI03 |
| Procesos de TI | ¿Se realiza un seguimiento a los cronogramas de actividades de los proyectos TIC?<br>¿Se documentan los inconvenientes evidenciados en la ejecución de cada uno de los proyectos de desarrollo? | APO04, APO05, DSS03 |

| | | |
|---|---|---|
| Direccionamiento Estratégico | ¿Se han definido roles y responsabilidades de los actores? | EDM03 |
| Equipo de Desarrollo | ¿Se han realizado sesiones de capacitación de forma regular respecto a los procesos, los roles y las responsabilidades de los actores?<br>¿Se realiza una adecuada transferencia de conocimiento a la gerencia? | APO07, APO08, BAI08 |
| Entrega del Producto | ¿Se toman medidas cuando el desempeño del software no está en el nivel requerido? | EDM05, APO12, APO13, BAI04, BAI06, DSS04 |

Con base a las respuestas para cada dominio en el instrumento, se debe hacer una posterior relación con el nivel de madurez propuesto por Cobit, para este ejemplo se tomará el dominio del equipo de desarrollo, así:

Tabla 3.
*Relación de Dominio, Pregunta y Nivel de Madurez*

| DOMINIO | PREGUNTAS | NIVEL DE MADUREZ |
|---|---|---|
| Equipo de Desarrollo | ¿Se han realizado sesiones de capacitación de forma regular respecto a los procesos, los roles y las responsabilidades de los actores? | Establecido |
| | ¿Se realiza una adecuada transferencia de conocimiento a la gerencia? | Gestionado |

Siguiendo la anterior metodología para establecer el contexto de la organización y el área de desarrollo de software, nos permitirá conocer la realidad actual para cada una de ellas.

Entrando a la segunda actividad que se refiere a la identificación de riesgos asociados al software Fénix, para la cual el área de desarrollo de software puede utilizar uno o varios enfoques teniendo en cuenta que, a mayor cantidad de fuentes de información, habrá mayor certeza en el listado de riesgos resultantes. Se recomiendan utilizar alguno de los siguientes mecanismos para la recolección del listado de riesgos asociados a la seguridad de la información para el software Fénix:

- Lluvia de ideas.
- Entrevistas.
- Talleres.
- Informes de auditoría.
- Análisis de incidencias reportadas en el software.
- Publicaciones en sitios web sobre riesgos en aplicaciones web.
- Lectura sobre estándares de gestión de riesgos de seguridad de la información.
- Lectura de normativas legales sobre el trato de datos personales.

Luego de la debida recolección de riesgos asociados a la seguridad de la información en el software Fénix, entramos a la actividad análisis de riesgos que se basa en determinar la probabilidad e impacto de estos a través de escalas de calificación cualitativa y cuantitativa. Esto para facilitar la posterior evaluación que permitirá clasificar los riesgos en el nivel correspondiente y así establecer la prioridad en la atención para cada riesgo.

En este punto de la fase dos, es importante tener en cuenta las capacidades y la experiencia que debe tener el personal encargado de ejecutar cada uno de los pasos del análisis de riesgos del software Fénix. Lo anterior con el objetivo de tener la información precisa para el análisis y que la respectiva evaluación se efectúe de manera objetiva y fundamentada.

Los talleres pueden ser una buena opción para realizar la evaluación de los riesgos del software Fénix, en estos talleres los participantes deben asignar una calificación cualitativa de, explotabilidad, prevalencia de vulnerabilidad, detectabilidad del riesgo, impacto técnico e impacto sobre el negocio, a cada uno de los riesgos considerados. Para realizar esta evaluación nos enfocamos en hacer uso de las buenas prácticas que nos ofrece el estándar OWASP.

Inicialmente se debe tener claridad sobre las variables para implementar la matriz de riesgos asociados a seguridad de la información según el estándar OWASP, así:

- Explotabilidad:

  revisa en el contexto de la seguridad de la información qué tan fácil es explotar la vulnerabilidad detectada.

- Prevalencia de la vulnerabilidad:

  busca como se puede corregir la vulnerabilidad o que tanto puede proseguir en el tiempo aun con modificación y actualización en el sistema vulnerable.

- Detectabilidad:

  Identifica qué tan fácil puede ser detectada la vulnerabilidad en el ambiente de trabajo y en internet.

- Impacto técnico:

  busca calificar qué impacto tendría en el sistema si la vulnerabilidad logra ser explotada.

- Impacto sobre el negocio:

  Owasp deja este ítem abierto para que cada compañía lo acoja o interprete según la experiencia y objetivos de negocio, y no lo incluye en el ámbito para la calificación final de la vulnerabilidad.

Así mismo, se debe tener en cuenta los criterios para evaluar cada una de las variables anteriormente descritas.

Se califica la explotabilidad, prevalencia y detectabilidad cada una en un rango de 1 a 3 y se promedian los 3 valores para después multiplicarlos por el impacto técnico que se califica según las métricas de CVSS que tienen una escala de 0 a 10 y luego por el impacto de negocio calificado de 0 a 30 (RAFAEL ENRIQUE RODRÍGUEZ RODRÍGUEZ, 2018).

Tabla 4.
*Variables y escala para calificar vulnerabilidad. Tomada de* (RAFAEL ENRIQUE RODRÍGUEZ RODRÍGUEZ, 2018)

| No | VARIABLE | ESCALA |
|---|---|---|
| 1 | Explotabilidad | De 0 – 3 |
| 2 | Prevalencia | De 0 – 3 |
| 3 | Detectabilidad | De 0 – 3 |
| 4 | Impacto técnico | De 0 – 10 |
| 5 | Impacto de negocio | De 0 – 30 |

Basándonos en la escala de criticidad para evaluar la vulnerabilidad, se debe emplear la siguiente regla para obtener el resultado total de la calificación para cada vulnerabilidad:

***((explotabilidad + prevalencia+ detectabilidad) /3) * impacto técnico) + impacto de negocio) /6***

Figura 3. Regla para obtener calificación de una vulnerabilidad. Tomado de (2018, p. 50)

En la Figura 3, se expone la forma como finaliza la matriz desarrollada con la metodología propuesta por el estándar OWASP.

| Riesgo | Agentes de Amenaza | Vectores de Ataque | Debilidades de Seguridad | | Impacto | | Puntuación |
|---|---|---|---|---|---|---|---|
| | | Explotabilidad | Prevalencia | Detectabilidad | Técnico | Negocio | |
| A1: 2017- Inyección | Específico de la Aplicación | FACIL: 3 | COMUN: 2 | FACIL: 3 | GRAVE: 3 | Específico de la Aplicación | 8,0 |
| A2: 2017 - Pérdida de Autenticación | Específico de la Aplicación | FACIL: 3 | COMUN: 2 | PROMEDIO: 2 | GRAVE: 3 | Específico de la Aplicación | 7,0 |
| A3: 2017 - Exposición de Datos Sensibles | Específico de la Aplicación | PROMEDIO: 2 | DIFUNDIDO: 3 | PROMEDIO: 2 | GRAVE: 3 | Específico de la Aplicación | 7,0 |
| A4: 2017 - Entidad Externa de XML (XXE) | Específico de la Aplicación | PROMEDIO: 2 | COMUN: 2 | FACIL: 3 | GRAVE: 3 | Específico de la Aplicación | 7,0 |
| A5: 2017 - Pérdida de Control de Acceso | Específico de la Aplicación | PROMEDIO: 2 | COMUN: 2 | PROMEDIO: 2 | GRAVE: 3 | Específico de la Aplicación | 6,0 |
| A6: 2017 - Configuración de Seguridad Incorrecta | Específico de la Aplicación | FACIL: 3 | DIFUNDIDO: 3 | FACIL: 3 | MODERADO: 2 | Específico de la Aplicación | 6,0 |
| A7: 2017 - Secuencia de Comandos en Sitios Cruzados (XSS) | Específico de la Aplicación | FACIL: 3 | DIFUNDIDO: 3 | FACIL: 3 | MODERADO: 2 | Específico de la Aplicación | 6,0 |
| A8: 2017 - Deserialización Insegura | Específico de la Aplicación | DIFICIL: 1 | COMUN: 2 | PROMEDIO: 2 | GRAVE: 3 | Específico de la Aplicación | 5,0 |
| A9: 2017 - Componentes con Vulnerabilidades Conocidas | Específico de la Aplicación | PROMEDIO: 2 | DIFUNDIDO: 3 | PROMEDIO: 2 | MODERADO: 2 | Específico de la Aplicación | 4,7 |
| A10: 2017 - Registro y Monitoreo Insuficientes | Específico de la Aplicación | PROMEDIO: 2 | DIFUNDIDO: 3 | DIFICIL: 1 | MODERADO: 2 | Específico de la Aplicación | 4,0 |

Figura 4 Ejemplo de matriz de riesgos, luego de implementar.

Una vez se obtengan los resultados de la calificación para cada vulnerabilidad en la escala de 0 a 10 como se ve en la Figura *4* Ejemplo de matriz de riesgos, luego de implementar., se

establece la calificación general del software ***Fénix,*** en cuanto a riesgos asociados a la seguridad de la información.

Tabla 5.
*Escala de calificación de vulnerabilidades según CVSS. Tomado de* (2018, pág. 51).

| Calificación | Escala |
|---|---|
| 0 | Nula |
| 0.1 - 3.9 | Baja |
| 4.0 - 6.9 | Media |
| 7.0 - 8.9 | Alta |
| 9.0 - 10 | Critica |

Con lo anterior, se da fin a la actividad de evaluación del riesgo asociado a la seguridad de la información en el software ***Fénix,*** y se da apertura a la actividad de tratamiento del riesgo que será articulado con las mejores prácticas a nivel de proceso catalizadores de Cobit 5. La base para el tratamiento de dichos riesgos radicará principalmente en el anexo A de la norma ISO 27001:2013, que provee de una forma organizada una lista de 114 controles (o medidas) de seguridad (Arévalo, 2020), de los cuales se obtienen 14 secciones se pueden utilizar para mejorar la seguridad de la información en el proyecto ***Fénix***.

Dentro de las 14 secciones que propone la norma podemos encontrar los siguientes (2020):

- Políticas de seguridad de la información (Control 5).
- Organización de la seguridad de la información (Control 6).
- Seguridad de los recursos humanos (Control 7).
- Gestión de recursos (Control 8).
- Control de acceso (Control 9).

- Criptografía (Control 10).
- Seguridad física y ambiental (Control 11).
- Seguridad Operacional (Control 12).
- Seguridad de las comunicaciones (Control 13).
- Adquisición, desarrollo y mantenimiento de sistemas (Control 14).
- Relaciones con los proveedores (Control 15).
- Gestión de incidentes en seguridad de la información (Control 16).
- Aspectos de seguridad de la información de la gestión de la continuidad del negocio (Control 17).
- Cumplimiento Legal (Control 18)

Cada uno de los controles destacados anteriormente, aporta significativamente a la protección del activo de la información en software Fénix. Los fundamentos del Anexo A de la norma ISO 27001, se pueden articular con los procesos encontrados en las buenas prácticas de Cobit ubicadas en el dominio de Alinear, planificar y organizar (APO) (Isaca, 2012, p. 24), más exactamente los proceso APO07, APO09, APO13.

Los procesos de cobit mencionados anteriormente, cubren en su mayoría el listado de control de la norma ISO 27001, agregándoles las buenas prácticas en cuanto a la gestión de los recursos humanos, es decir, para cobit es fundamental que el recurso humano participante dentro del proyecto Fénix, esté alineado a las TI y estrategias del negocio. Una de las buenas prácticas relevantes de Cobit que impactaría en la seguridad de la información, es la de garantizar el entrenamiento del personal implicado en el proyecto, con el fin de reducir la dependencia de una

sola persona en la ejecución de actividades enfocadas a la seguridad del software. También se debe evaluar constantemente el desempeño laboral respecto a los objetivos establecidos en el proyecto para evitar retrasos y brechas de seguridad.

Para el proceso APO09 relacionado con los acuerdos de servicios, es necesario realizar una lista de chequeo donde se valide el catálogo de servicios de TI relacionados al tratamiento de los datos personales y otra información que son ofrecidos al cliente externo, esto con el fin de no dejar cabos sueltos que a corto a largo plazo represente un riesgo para el cliente y la organización considerando temas legales.

La gestión de la seguridad inmersa en el proceso APO13 de Cobit, está enfocada a mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo (Isaca, 2012, p. 113). Para ello se debe ejecutar un plan consistente de soluciones de seguridad de la información, como la instalación de sistemas de control, sistemas de seguridad informática, para que la información del cliente se encuentre disponible y a salvo en cualquier momento. Una de las prácticas recomendadas en este proceso es que se garantice el cronograma de soportes en el aplicativo, también que se garantice el uso adecuado del software, para esto se debe crear una campaña de conciencia sobre el uso de herramientas de arquitectura web.

Como última actividad del proceso de gestión de riesgos de seguridad de la información encontramos la aceptación del riesgo. El nivel de aceptación debe estar basado en la evaluación que fue desarrollada anteriormente, para esto el área de desarrollo encargada del proyecto Fénix necesita establecer un rango de tolerancia sobre los riesgos, basados en la experiencia y documentación previamente estructurada.

Una vez finalizada las fases del proceso de gestión de riesgos de seguridad de la información para el proyecto Fénix, nos encontramos con dos procesos transversales que son la comunicación del riesgo y el monitoreo y revisión del riesgo. Estos procesos se deben realizar de forma continua por medio de revisiones y reuniones semanales para evaluar los avances que ha tenido el proyecto Fénix.

## 2.2 Sistematización de datos obtenidos.

En el departamento de TI específicamente en el área de desarrollo de software la cual está encargada del proyecto de software Fénix, se realizó la dinámica de lluvia de ideas y una búsqueda exhaustiva en la web para identificar los riesgos que estaban asociados a la seguridad de la información en el proyecto, obteniendo una lista de amenazas, vulnerabilidades y riesgos, donde posteriormente se evaluaron 3 riesgos utilizando la metodología de evaluación propuesta por el estándar OWASP.

Las amenazas identificadas son relacionadas a continuación:

Tabla 6.
*Listado de amenazas encontradas*

| AMENZAS | | |
|---|---|---|
| DE INFORMACION | A1 | Comprometer información confidencial. |
| | A2 | Destrucción de registros. |
| | A3 | Revelación de información. |
| | A4 | Divulgación de contraseñas. |
| | A5 | Falsificación de registros. |
| | A6 | Espionaje industrial. |
| | A7 | Fuga de información. |
| | A8 | Uso indebido de los sistemas de información. |
| | A9 | Cambio involuntario de datos en un sistema de información. |
| | A10 | Cambios no autorizados de registros. |
| | A11 | Error de usuario. |
| INFRAESTRUCTURA | A12 | Fallo de los enlaces de comunicación. |
| | A13 | Mal funcionamiento del equipo. |
| SOFTWARE | A14 | Acceso a la red o al sistema de información por personas no autorizadas. |
| | A15 | Infracción legal. |
| | A16 | Ocultar la identidad de un usuario. |
| | A17 | Daño causado por un tercero. |
| | A18 | Daños resultantes de las pruebas de penetración. |
| | A19 | Errores en mantenimiento. |
| | A20 | Código malicioso. |
| | A21 | Errores de software. |
| | A22 | Instalación no autorizada de software. |

Las vulnerabilidades se relacionan a continuación:

Tabla 7.
Listado de Vulnerabilidades encontradas

| VULNERABILIDADES | | |
|---|---|---|
| DE INFORMACION | V1 | No validación de los datos procesados. |
| | V2 | Uso incontrolado de sistemas de información. |
| | V3 | No uso de api's para separar los datos de los comandos y la consulta |
| INFRAESTRUCTURA | V4 | Eliminación de medios de almacenamiento sin eliminar datos. |
| | V5 | Inadecuada gestión de capacidad del sistema. |
| SOFTWARE | V6 | Interfaz de usuario complicada. |
| | V7 | Gestión inadecuada del cambio. |
| | V8 | Mantenimiento inadecuado. |
| | V9 | Inadecuada gestión y protección de contraseñas. |
| | V10 | Pruebas de software insuficientes. |
| | V11 | Ausencia de sistemas de identificación y autenticación. |
| | V12 | Descarga no controlada de Internet. |
| | V13 | Software no documentado. |
| | V14 | Los permisos del usuario no se revisan regularmente. |

Los 3 riesgos evaluados fueron los siguientes:

Tabla 8.
Listado de riesgos evaluados

| MUESTRA DE RIESGOS | | |
|---|---|---|
| AMENAZA | VULNERAVILIDAD | RIESGOS |
| A3 | V3 | Inyección de datos no confiables a un interprete como parte de un comando de consulta |
| A1 | V12 | Exposición de datos sencibles |
| A14 | V14 | Pérdida de control de acceso |

Luego de la aplicación de la metodología propuesta por el estándar OWASP para la gestión de riesgos asociados a seguridad de la información orientadas al proyecto Fénix, la siguiente fue la matriz resultante:

| RIESGOS IDENTIFICADOS | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| AMENAZA | VULNERAVILIDAD | RIESGOS | EXPLOTABILIDAD | PREVALENCIA | DETECTABILIDAD | IMPACTO TECNICO | IMPACTO DE NEGOCIO | PUNTUACION |
| A3 | V3 | Inyección de datos no confiables a un interprete como parte de un comando de consulta | 3 | 1 | 1 | 10 | 30 | 8 |
| A1 | V12 | Exposición de datos sencibles | 3 | 3 | 2 | 10 | 30 | 9 |
| A14 | V14 | Perdida de control de acceso | 3 | 1 | 2 | 10 | 30 | 8 |
| | | | | | | NIVEL DE VULNERABILIDAD DEL SITIO | | 9 |

Figura 5. Matriz resultante luego de la aplicación de metodología del estándar OWASP. Fuente: creación propia.

# 3 RESULTADOS

## 3.1 Identificación y análisis de las alternativas de solución.

En el proceso de identificación de las alternativas de solución, encontramos la guía de gestión de riesgos de seguridad y privacidad de la información propuesta por el ministerio de tecnología y comunicaciones que de igual forma está basada en la norma técnica NTC ISO/IEC 27001. En esta guía se plasman todas las referencias a políticas, definiciones y contenido relacionado que apoya la toma de decisiones.

Esta alternativa toma como punto vital, la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación alta dependiente de los criterios de confidencialidad, integridad y disponibilidad. Sin embargo, esta guía de gestión de riesgos expresa una visión muy general en

cuanto a la identificación, evaluación y tratamiento de los riesgos, es decir, no afecta directamente el área de desarrollo de software.

La guía de gestión de riesgos de seguridad y privacidad de la información que propone el ministerio de tecnologías de la información y comunicaciones, no se articula con algún otro marco de trabajo o estándar, esto deja brechas abiertas que pueden ser abordadas por mejores prácticas si estuviera articulada. Además, esta no incluye el establecimiento de un gobierno de TI y asignación de roles a los participantes de este.

También la guía de gestión de riesgos de seguridad y privacidad de la información deja por fuera la actividad de la aceptación del riesgo, llegando solamente hasta el tratamiento de este.

Por lo anterior se desarrolló en este estudio de caso una metodología que articula el marco de trabajo Cobit 5 con las normativas ISO 27001, ISO/IEC 27005, y el estándar OWASP para atacar todas estas brechas en cuanto a seguridad de la información que posee el software Fénix, también apoyará la alineación de los objetivos y estrategias de la organización con el área de desarrollo.

La articulación de los marcos y normativas mencionados anteriormente nos permitirá abordar desde el conocimiento inicial del estado actual de la organización y del área de desarrollo, hasta el tratamiento y aceptación de los riesgos asociados a seguridad de la información.

Se llegó a determinar con el análisis según la metodología propuesta en este estudio de caso, que la gestión de los riesgos asociados a seguridad de la información del software Fénix que encontramos en la Figura 7, que se están dejando pasar por alto la implementación de estándares que permitan minimizar la aparición e impacto de riesgos asociados de la seguridad de la información.

### 3.2 Selección de alternativas de solución y plan de acción.

La solución factible para abordar los temas relacionados a la gestión de riesgos de seguridad de la información del software Fénix, es la metodología propuesta en este caso de estudio ya que permitirá abordar desde muchos ángulos el correcto tratamiento de los datos personales del cliente externo.

El respectivo plan de acción sería la aplicación de la metodología planteada en este estudio de caso, ya que permite a través de la articulación de varios marcos y estándares la identificación, la evaluación, el tratamiento y la aceptación de los riesgos. Así mismo el establecimiento del gobierno dentro del área de desarrollo de software de la organización.

## 4. REFERENCIAS BIBLIOGRÁFICAS

### Bibliografía

Arévalo, M. C. (13 de Octubre de 2020). *Opirani*. Obtenido de https://www.piranirisk.com/es/blog/cuantos-controles-tiene-la-norma-iso-27001

Avdoshin, S. M., & Pesotskaya, E. Y. (2011). Software risk management . *2011 7th Central and Eastern European Software Engineering Conference (CEE-SECR)*(10.1109/CEE-SECR.2011.6188471), 1-6.

COLOMBIA, E. C. (17 de Octubre de 2012). LEY ESTATUTARIA 1581 DE 2012. Bogotá. Obtenido de https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf

Foundation, T. O. (2013). *OWASP top 10 - 2013 Los diez riesgos mas criticos en aplicaciones web.* Maryland: Creative Commons Attribution ShareAlike.

H. (06 de 2015). *Bonnadona Prevenir | Misión - Visión.* Obtenido de Organización Clínica Bonnadona Prevenir: https://www.organizacioncbp.org/mision.php

Isaca. (2012). *blplegal.* Obtenido de http://blplegal.net/zoneSite/RestFulApiZoneSite/uploads/1539031830-Cobit%205%20-%20Procesos%20Catalizadores.pdf

Isaca. (2012). COBIT 5.0. Enabling Processes. *Isaca (2012)*. Estados Unidos.

Isaca. (2012). COBIT 5.0. Un marco de negocio para el gobierno y la gestión de TI de la empresa. *Isaca (2012)*. Estados Unidos.

Isaca. (2012). *ucipfg.* Obtenido de https://www.ucipfg.com/Repositorio/MATI/MATI-01/Unidad4/lecturas/51855611-Risk-IT-Framework-Espanol.pdf

Marlene Lucila Guerrero Julio, C. U. (25 de Septiembre de 2019). Evaluación del contexto organizacional en la gestión del riesgo de tecnología de información con un enfoque basado en COBIT. *RITI Journal*, 4. doi:https://doi.org/10.36825/RITI.07.14.004

RAFAEL ENRIQUE RODRÍGUEZ RODRÍGUEZ, A. F. (2018). DESARROLLO DE UN MODELO PARA CALCULAR EL NIVEL DE SEGURIDAD EN SITIOS WEB, BASADO EN EL TOP 10 DE VULNERABILIDADES MÁS EXPLOTADAS EN 2017 SEGÚN EL MARCO DE REFERENCIA OWASP. *DESARROLLO DE UN MODELO PARA CALCULAR EL NIVEL DE SEGURIDAD EN SITIOS WEB, BASADO EN EL TOP 10 DE VULNERABILIDADES MÁS EXPLOTADAS EN 2017 SEGÚN EL MARCO DE REFERENCIA OWASP*, 48-51. Bogotá, Colombia.

Tao, Y. (12 de 08 de 2008). A STUDY OF SOFTWARE DEVELOPMENT PROJECT RISK MANAGEMENT. *2008 International Seminar on Future Information Technology and Management Engineering*, (pág. 1). Leicestershire. doi:10.1109/FITME.2008.125